UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

RON PROSKY, individually, and on behalf of all others similarly situated, Plaintiff, v. PALM BEACH HEALTH NETWORK PHYSICIAN GROUP D/B/A PALM BEACH HEALTH NETWORK, and PALM BEACH GARDENS COMMUNITY HOSPITAL, INC. D/B/A PALM BEACH GARDENS MEDICAL CENTER, Defendants.	**Case No.:** 9:24cv80656 **Class Action** **Jury Trial Demanded**

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Ron Prosky ("**Plaintiff**"), individually and on behalf of the proposed Class defined herein, alleges the following against Defendants Palm Beach Health Network Physician Group d/b/a Palm Beach Health Network ("PBHN") and Palm Beach Gardens Community Hospital, Inc. d/b/a Palm Beach Gardens Medical Center ("PBGMC") (together, "**Defendants**"). Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys.

INTRODUCTION

1. The Palm Beach Health Network is the largest healthcare network in Palm Beach County. [1] PBHN includes a large multi-specialty physician group, ambulatory surgery centers,

[1] https://www.palmbeachhealthnetwork.com/about/leadership-team

outpatient diagnostic facilities and six hospitals and care centers throughout Palm Beach County, Florida, including:

- Delray Medical Center
- Good Samaritan Medical Center
- Palm Beach Children's Hospital
- St. Mary's Medical Center
- West Boca Medical Center
- Palm Beach Gardens Medical Center

2. PBGMC is a 199-bed acute care hospital providing medical and surgical services. PBGMC offers advanced orthopedic and joint replacement care, a primary stroke center, diagnostic imaging, general and robotic surgery, urology, epilepsy monitoring and 24-hour emergency care.[2]

3. This case arises from Defendants' systematic violation of the medical privacy rights of its patients by exposing their highly sensitive personal information without their patients' knowledge or consent, through the use of the Meta Platform Inc. d/b/a Facebook ("**Meta**" or "**Facebook**") tracking and collection tools.

4. Defendants operate several websites including https://www.pbgmc.com/ and https://www.palmbeachhealthnetwork.com/ ("**Websites**") and "My Health Rec" Patient Portal, available at https://www.pbgmc.com/portal (the **"Portal"**) (and collectively with the Websites, the "**Web Properties**").[3]

[2] https://www.pbgmc.com/about/about-pbgmc

[3] Upon information and good faith belief, all login pages for various PBHM entities and their websites' patient portals, including PBGMC, also get routed to https://palmbeachhealthnetwork.myhealth-rec.com.

5. Defendants invite their patients to use their Web Properties to seek medical care and to share their personal and health information in the process.

6. As detailed herein, Defendants have disregarded the privacy rights of their patients who used their Web Properties ("**Users**" or "**Class Members**") by intentionally, willfully, recklessly and/or negligently failing to implement adequate and reasonable measures to ensure that the Users' personally identifiable information ("**PII**") and protected health information ("**PHI**") (collectively, "**Private Information**") was safeguarded.

7. Unbeknownst to Users and without those Users' authorization or informed consent, Defendants installed Facebook's Meta Pixel ("**Meta Pixel**" or "**Pixel**") and other invisible third-party tracking technology, on its Websites in order to intercept Users' PII and PHI with the express purpose of disclosing that Private Information to third parties such as Meta and/or Google LLC in violation of the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") Privacy Rule and 42 U.S.C. § 1320d-6 as well as state, federal and common law.

8. Meta then improperly accesses and uses the Private Information for their benefit. Meta associates the Private Information received with the individual User whose information was disclosed and creates targeted advertising that it sends to that User's personal Facebook accounts.

9. Meta encourages businesses like Defendants to use the Pixel and intentionally bypasses any opt out features for Users in order to extract valuable data for marketing purposes because Meta's revenue is derived almost entirely from selling targeted advertising. Meta does not offer any tools to the affected Users and patients to opt out of such extensive tracking; even the most sophisticated Users who enable cookie blockers cannot avoid having their information tracked through the various Meta tracking tools.

10. Meta is able to personally identify each User with an active Facebook account by

using the "c_user" cookie that Meta stores in users' browsers and which reveals a Facebook account-holder's unique "FID" value. A user's FID is linked to their Facebook profile, which personally identifies the user through a wide range of demographic and other information about the user, including the user's name, pictures, personal interests, work history, relationship status, and other details. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to quickly and easily locate, access, and view the user's corresponding Facebook profile.[4]

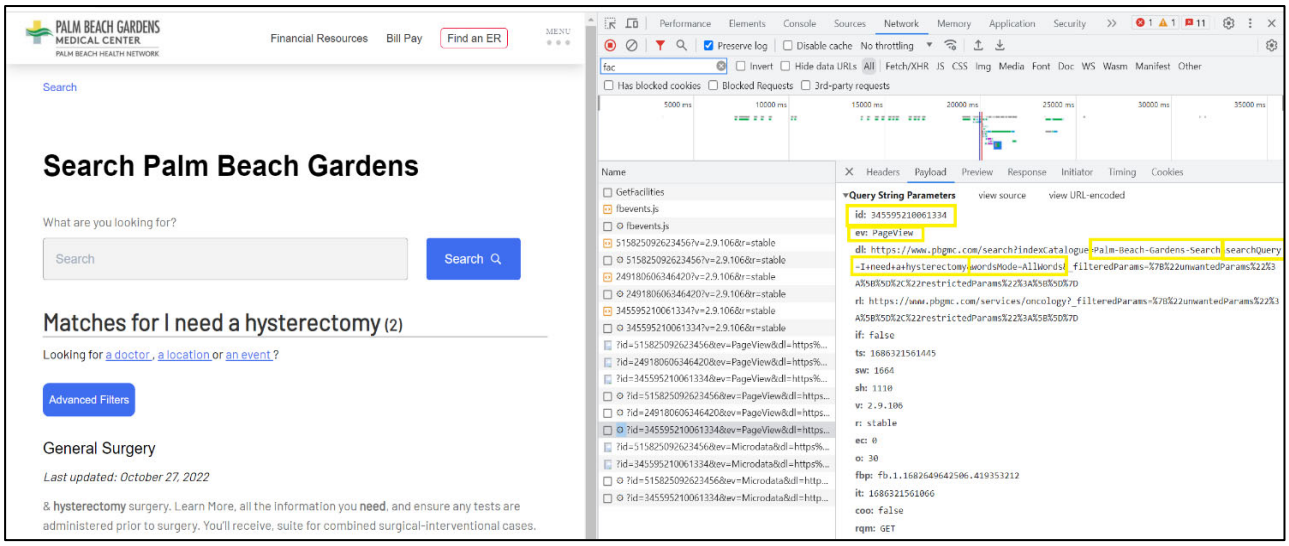
11. However, the Pixel collects data regardless of whether the Website visitor has a Facebook account. In fact, Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Pixel to the user's real-world identity using their shadow profile.[5]

12. The screenshots of Defendants' Websites, more fully explained *infra*, demonstrate how the Meta Pixel intercepts Users' Private Information, including the Private Information of Plaintiff and Class Members.

[4] To find the Facebook account associated with a particular c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

[5] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited May 21, 2024).

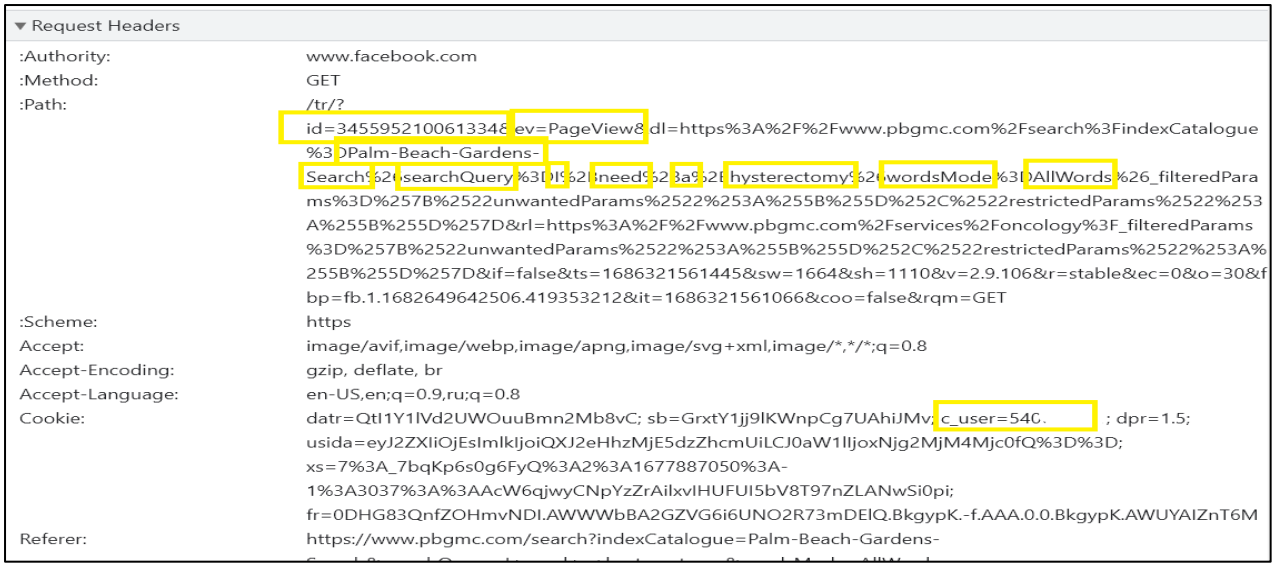
13. The first screenshot below shows what a webpage from Defendants' Websites looks like and how the Pixel works to disclose information to Meta.



14. On the left-hand side of the screenshot is the page as it appears to any User visiting this webpage. This is the result the User would see if they went to the Website's search bar, typed in "I need a hysterectomy" and pressed Enter. There are two matches for that search on Defendants' Website.

15. The right-hand side of the screenshot reveals what information Defendants are disclosing to Meta through the Pixel unbeknownst to the User.

16. This is further evidenced by the image below, which was collected during the same browsing session as the previous image. Though it appears to be code, a closer inspection makes it apparent that Defendants are disclosing both personally identifiable information in the form of the c_user FID, which uniquely identifies an individual's Facebook account (as well as other cookies that Facebook is known to utilize to identify individuals), as well as PHI that the User is sharing with Defendants when they use the Website.



▼ Request Headers

:Authority:	www.facebook.com
:Method:	GET
:Path:	/tr/? id=3455952100613348&ev=PageView&dl=https%3A%2F%2Fwww.pbgmc.com%2Fsearch%3FindexCatalogue%3DPalm-Beach-Gardens- Search%26searchQuery%3DI%2Bneed%2Ba%2Bhysterectomy%26wordsMode%3DAllWords%26_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522restrictedParams%2522%253A%255B%255D%257D&rl=https%3A%2F%2Fwww.pbgmc.com%2Fservices%2Foncology%3F_filteredParams%3D%257B%2522unwantedParams%2522%253A%255B%255D%252C%2522restrictedParams%2522%253A%255B%255D%257D&if=false&ts=1686321561445&sw=1664&sh=1110&v=2.9.106&r=stable&ec=0&o=30&fbp=fb.1.1682649642506.419353212&it=1686321561066&coo=false&rqm=GET
:Scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9,ru;q=0.8
Cookie:	datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv; c_user=540[redacted]; dpr=1.5; usida=eyJ2ZXIiOjEsImlkIjoiQXJ2eHhzMjE5dzZhcmUiLCJ0aW1lIjoxNjg2MjM4Mjc0fQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcW6qjwyCNpYzZrAilxvIHUFUI5bV8T97nZLANwSi0pi; fr=0DHG83QnfZOHmvNDI.AWWWbBA2GZVG6i6UNO2R73mDElQ.BkgypK.-f.AAA.0.0.BkgypK.AWUYAIZnT6M
Referer:	https://www.pbgmc.com/search?indexCatalogue=Palm-Beach-Gardens-

17. The highlighted portions reveal the information that Defendants are sharing with Meta. Beginning at the top, the "id=345595…" is the unique ID number of the Pixel installed by Defendants. Next to that is "PageView," a type of 'event' collected by the Pixel as the User navigates the Website and which shares the URL of the page that the User is visiting. Finally, on the top line, Defendants are disclosing that the User is visiting "www.pbgmc.com."

18. On the next line, Defendants discloses to Meta the PHI of the User. Here, Defendants are disclosing that the User performed a "search" and the "searchQuery" they typed in for that search was "I need a hysterectomy." Now Meta knows that the User is searching for information related to the Users' need for a hysterectomy, personal health information that is protected by HIPAA.

19. The last highlighted line, which begins with "cookies," contains the PII disclosed to Meta that allows Meta to specifically associate the PHI shared in the earlier lines with a specific individual.

20. Specifically, the highlighted "c_user" cookie followed by the number "54…" contains the unique Facebook User ID for the person visiting this webpage. This user ID, or FID, can be used to find the user's Facebook account. If you have a person's FID, all you have to do is

add it to the Facebook URL to find the profile.

21. In other words, with the use of the Pixel it installs on its Web Properties, Defendants intercept both the PII and the PHI of every User that visits every webpage, with the specific purpose of disclosing that HIPAA-protected health information to Meta.

22. Meta, which created the Pixel and assigns a unique FID to each of its Facebook account holders, knows how to combine the information intercepted and shared by Defendants so that Meta can connect each User to the PHI that is disclosed. Meta does this in order to send targeted advertisements related to the medical conditions and treatments each User shares with Defendants to that User's personal Facebook account.

23. The Pixel intercepts and discloses the information of every Facebook user that visits Defendants' Websites in the same way. So when Plaintiff and Class Members visited Defendants' Website, the URLs that describe the medical information on each page they visited (for example: https://www.pbgmc.com/search) and/or the search terms they typed in Defendants' search bar were simultaneously shared with Meta. Together with that PHI, Defendants' Pixel (which relies on Facebook cookies to function) discloses to Meta the Facebook ID of every person that visits its Website so that Meta can personally identify that User and that User's PHI—including Plaintiff and every Class Member who visited Defendants' Websites to research and share HIPAA-protected health information with Defendants while the Pixel was installed on the Website.

24. Plaintiff and Class Members who used Defendants' Websites thought they were communicating with only their trusted healthcare providers, and reasonably believed that their sensitive and private PHI would be guarded with the utmost care. In browsing Defendants' Websites—to locate and make an appointment with a doctor, find sensitive information about their diagnosis, or investigate treatment—Plaintiff and Class Members did not expect that every search

(including exact words and phrases they typed into search bars), sensitive PHI such as health conditions (e.g., stroke), diagnoses (e.g., epilepsy), procedures sought and/or the names and locations of physicians, would be intercepted, captured and otherwise shared with Facebook in order to target Plaintiff and Class Members with ads, in conscious disregard of their privacy rights.

25. Plaintiff continued to have his privacy violated when his Private Information was used to turn a profit by way of targeted advertising related to his medical conditions and treatments sought.

26. Defendants knew that by embedding the Meta Pixel on their Websites they were enabling Facebook to collect and use Plaintiff's and Class Members' Private Information, including sensitive medical information.

27. Defendants (or any third parties) did not obtain Plaintiff's and Class Members' prior consent before sharing their sensitive, confidential communications with third parties such as Facebook.

28. Defendants' actions constitute an extreme invasion of Plaintiff's and Class Members' right to privacy and violate federal and state statutory and common law as well as Defendants' own Privacy Policies that affirmatively and unequivocally state that any personal information provided to Defendants will remain secure and protected.[6]

29. As a result of Defendants' conduct, Plaintiff and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with doctors online; (iii) emotional distress and heightened concerns related to the release of Private

[6] Defendants' Privacy Policies (and other affirmative representations) represent to Users that it will not share Private Information with third parties without the patient's consent. *See* Privacy Policy, PALM BEACH HEALTH NETWORK, https://www.palmbeachhealthnetwork.com/privacy-policy (last visited May 21, 2024).

Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information. Plaintiff and Class Members have a substantial risk of future harm, and thus injury in fact, due to the continued and ongoing risk of misuse of their Private Information that was shared by Defendants with third parties.

30. Plaintiff seeks, on behalf of himself and a class of similarly situated persons, to remedy these harms and therefore asserts the following claims against Defendants: (i) Violation of the Florida Security of Communications Act ("**FSCA**"), Fla. Stat. 934.01, *et seq*.; (ii) Violation of the Florida Deceptive and Unfair Trade Practices Act ("**FDUTPA**"), Fla. Stat. § 501.201, *et seq*.; (iii) Violation of Electronic Communications Privacy Act, 18 U.S.C. §2511, *et seq.* ("**ECPA**"); (iv) Invasion of Privacy; (v) Breach of Implied Contract; (vi) Negligence; (vii) Breach of Confidence; (viii) Breach of Fiduciary Duty; and (ix) Unjust Enrichment.

PARTIES

31. Plaintiff Ron Prosky was a Florida resident at all relevant times, including at least until late 2021.

32. Defendant Palm Beach Gardens Community Hospital, Inc., d/b/a Palm Beach Gardens Medical Center is a for-profit company incorporated in Florida and located at 3360 Burns Rd., Palm Beach Gardens, FL 33410.

33. Defendant Palm Beach Health Network Physician Group d/b/a Palm Beach Health Network is a for-profit company incorporated in Florida and located at 8794 Boynton Beach Blvd #103, Boynton Beach, FL 33472.

JURISDICTION & VENUE

34. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under a law of the United States (*i.e.*, the ECPA).

35. This Court also has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

36. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. Plaintiff is a citizen of Florida, resides in this District, and used Defendants' Web Properties within this District. Moreover, Defendants receive substantial compensation from offering healthcare services in this District, and Defendants made numerous misrepresentations which had a substantial effect in this District, including, but not limited to, representing that they will only disclose Private Information provided to them under certain circumstances, ***which do not*** include disclosure of Private Information for marketing purposes.

37. Defendants are subject to personal jurisdiction in Florida based upon sufficient minimum contacts which exist between Defendants and Florida. Defendants are incorporated in Florida and are conducting business in Florida.

REPRESENTATIVE PLAINTIFF'S EXPERIENCES

Plaintiff Ron Prosky

38. Plaintiff Prosky began receiving healthcare services from PBGMC in 2019 and continued until mid-2021. Plaintiff Prosky utilized Defendant Palm Beach Gardens Medical Center Website and Patient Portal ("**PBGMC Web Properties**") in connection with said services.

39. Defendants encouraged Plaintiff Prosky to utilize PBGMC's Web Properties to search for doctors, make appointments, review medical treatments, and to review his medical records.[7]

40. While using PBGMC Web Properties, Plaintiff Prosky communicated sensitive—and what he expected to be confidential—personal and medical information to Defendants.

41. Plaintiff Prosky used PBGMC Web Properties to research healthcare providers (including [redacted]) and communicate with them, research particular medical concerns and treatments including imaging, fill out forms and questionnaires, schedule and attend appointments [redacted], and perform other tasks related to his specific medical inquiries and treatment.

42. Plaintiff Prosky also utilized PBGMC's [redacted].

[7] *See, e.g.*, *Welcome to My Health Rec, Our Patient Portal*, PALM BEACH HEALTH NETWORK, https://www.pbgmc.com/portal (last visited May 21, 2024) ("My Health Rec is a great way to view, download and transmit your up-to-date health information, all from the convenience and privacy of your own home, or anywhere Internet access is available — 24 hours a day, seven days a week. We recently added opportunities for additional documents you can see online, such as pathology reports, discharge summaries and progress/procedure notes").

43. Plaintiff Prosky also utilized PBGMC's Patient Portal to look at his bills and payments, to make appointments with his treating physicians, and to see his test results and notes from his appointments.

44. While using PBGMC's digital services, Plaintiff Prosky communicated and received information regarding his appointments, treatments, medications, and clinical information, including his imaging results. As a result of the Meta Pixel Defendants chose to install on their Web Properties, this information was intercepted, viewed, analyzed, and used by unauthorized third parties.

45. Plaintiff Prosky accessed PBGMC's Web Properties in connection with receiving healthcare services from PBGMC or PBGMC's affiliates at PBGMC's direction and with PBGMC's encouragement.

46. Plaintiff has used and continues to use the same devices to maintain and to access an active Facebook account throughout the relevant period in this case.

47. As a medical patient using PBGMC's health services, Plaintiff Prosky reasonably expected that his online communications with PBGMC were solely between himself and PBGMC, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Prosky also relied on Defendant PBGMC's Privacy Policies and reasonably expected that PBGMC would safeguard his Private Information. But for his status as Defendants' patient and Defendants' representations via its Privacy Policies, Plaintiff Prosky would not have disclosed his Private Information to Defendants.

48. Plaintiff Prosky is also an active Facebook user and has had a Facebook account since at least 2009.

49. Plaintiff Prosky used the same e-mail address to sign up for a Facebook account and for PBGMC's Patient Portal.

50. As a result of Defendants' use of the Meta Pixel, Plaintiff Prosky began receiving advertisements on Facebook relating to his particular medical conditions and treatments, including: [redacted]

51. During his time as PBGMC's patient, Plaintiff Prosky never consented to the use of his Private Information by third parties or to Defendants enabling third parties, including Facebook, Google, and others to access or interpret such information.

52. Upon information and good faith belief, Plaintiff began receiving these ads after his PII and PHI concerning his medical conditions, including his [redacted] was disclosed by Defendants through the Pixel to Meta. Meta then viewed and accessed this Private Information so that it could personally identify Plaintiff by connecting his c_user FID to his Facebook account. Meta also accesses the PHI disclosed by Defendants so that it can use the specific medical information Plaintiff shared with Defendants, including the specialty and locations of his treating physicians, to identify specific targeted ads related to Plaintiff's medical condition and perceived medical needs to send to his Facebook account. After accessing and identifying the specific medical conditions and other protected health information it can target with ads, Meta then shares that information with *additional* unauthorized third parties whose businesses and advertisements are related to those conditions.

53. The full scope of Defendants' interceptions and disclosures of Plaintiff's communications to Meta can only be determined through formal discovery. However, Defendants

intercepted at least the following communications about Plaintiff's prospective healthcare providers. The following long-URLs or substantially similar URLs were sent to Meta via the Pixel:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

54. Notwithstanding, through the Meta Pixel and similar tracking technologies embedded on PBGMC's Web Properties, Defendants transmitted Plaintiff Prosky's Private Information to third parties, including Facebook, Google, and others.

55. Plaintiff Prosky would not have utilized Defendants' medical services and/or used its Web Properties or would have paid much less for Defendants' services had he known that his Private Information would be captured and disclosed to third parties like Facebook without his consent.

FACTUAL BACKGROUND

A. Defendants Irresponsible Use of Invisible Tracking Codes by Healthcare Providers to Send Meta People's Data for its Advertising Business.

56. Meta operates the world's largest social media company whose revenue is derived almost entirely from selling targeted advertising.

57. The Meta Pixel and other third-party tracking tools also collect and transmit information from Defendants that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Facebook encourages its healthcare Partners to use, including uploading patient lists to Facebook for use in its advertising systems.

58. Meta associates the information it obtains via the Meta Pixel with other information regarding the User, using personal identifiers that are transmitted concurrently with other information the Pixel is configured to collect. For Facebook account holders, these identifiers include the "c_user" cookie IDs, which allow Meta to link data to a particular Facebook account. For both Facebook account holders and users who do not have a Facebook account, these identifiers also include cookies that Meta ties to their browser.

59. Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a "completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads." [8]

60. One of its most powerful advertising tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

61. Ad Targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico." [9]

[8] *Facebook Unveils Facebook Ads*, META (November 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

[9] Natasha Singer, *What You Don't Know about How Facebook Uses Your Data* (April 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

62. The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their website to "measure, optimize and build audiences for … ad campaigns."[10]

63. Meta describes the Pixel as "a snippet of Javascript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook accounts.[11]

64. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[12]

65. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

b. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[13]

[10] *Meta Pixel* (2023), https://web.archive.org/web/20231219015131/https://www.facebook.com/business/tools/meta-pixel (last visited May 21, 2024).

[11] *Meta Pixel* (2023), https://developers.facebook.com/docs/meta-pixel/.

[12] *Meta Pixel* (2023), https://www.facebook.com/business/tools/meta-pixel.

[13] *Id.*

Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

66. Meta explains that the Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

67. The Meta Pixel is customizable and web developers can choose the actions the Pixel will track and measure on a particular webpage.

68. Meta advises web developers to place the Pixel early in the source code17[14] for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.[15]

69. Meta's "Health" division is dedicated to marketing to and servicing Meta's healthcare "Partners." Meta defines its "Partners" to include businesses that use Meta's products,

[14] Source code is a collection of instructions (readable by humans) that programmers write using computer programming languages such as JavaScript, PHP, and Python. When the programmer writes a set or line of source code, it is implemented into an application, website, or another computer program. Then, that code can provide instructions to the website on how to function. *What is Source Code & Why Is It Important?* (July 19, 2023), https://blog.hubspot.com/website/what-is-source-code (last visited May 21, 2024).

[15] *Meta Pixel: Get Started* (2023), *https://developers.facebook.com/docs/meta-pixel/get-started*.

including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

70. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

71. Healthcare providers like Defendants encourage Plaintiff and Class Members to access and use various digital tools via its Web Properties to, among other things, receive healthcare services, in order to gain additional insights into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

72. In exchange for installing the Pixels, Facebook provided Defendants with analytics about the advertisements it has placed as well as tools to target people who have visited its Web Properties.

73. Upon information and belief, Defendants and other companies utilized Plaintiff's and Class Members' sensitive information and data collected by the Meta Pixels on Defendants' Web Properties in order to advertise to these individuals later on Meta's social platforms.

74. If a healthcare provider, such as Defendant, installs the Pixel as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. For example, when a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the communication to Meta while the patient is communicating with his or her healthcare provider. In other words, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

75. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing,"[16] which in this case included the content of Defendants' patients' communications with its Web Properties, including their PHI.

76. For Facebook, the Pixel acts as a conduit of information, sending the information it collects to Facebook through scripts running in the User's internet browser, via data packets labeled with PII, including the User's IP address, the Facebook c_user cookie and third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.[17]

77. Facebook's access to use even only some of these data points—such as just a "descriptive" webpage URL—is problematic. As Laura Lazaro Cabrera, a legal officer at Privacy International, explained: "Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data."[18]

78. The collection and use of this data raises serious privacy concerns and the potential misuse of personal information. For example, when Users browse Defendants' Web Properties, every step of their activity, click, keystroke, is tracked and monitored, including the specialties

---

[16] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything* (March 4, 2020), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/.

[17] The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users. *See* Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech* (June 8, 2022), https://clearcode.cc/blog/facebook-first-party-cookie-adtech/.

[18] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Sept. 25, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

and locations of treating and other physicians. By analyzing this data using algorithms and machine learning techniques, Facebook (and other entities tracking this information) can learn a chilling level of detail about Users' medical conditions, behavioral patterns, preferences, and interests.

79. This data can be used not only to provide personalized and targeted content and advertising, but also for more nefarious purposes, such as tracking and surveillance. Moreover, the misuse of this data could potentially lead to the spread of false or misleading information, which could have serious consequences, particularly in the case of health-related information.[19]

80. As pointed out by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), impermissible disclosures of such data in the healthcare context "may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI…. This tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment."[20]

81. Unfortunately, several recent reports detail the widespread use of third-party tracking technologies on hospitals', health care providers' and telehealth companies' digital

[19] *See e.g.*, Knvul Sheikh, *Your Health Information Was Hacked. What Now*, THE NEW YOUR TIMES (Dec. 7, 2023), https://www.nytimes.com/article/health-data-breach.html#:~:text=For%20people%20whose%20information%20is%20leaked%2C%20a%20breach,enterprise%20data%20and%20analytics%20at%20NYU%20Langone%20Health. ("For people whose [health] information is leaked, a breach can violate patient privacy and put them at risk of identity theft, insurance fraud or discrimination if, for example, their treatment for a stigmatized condition such as addiction or AIDS is made public…").

[20] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited May 21, 2024).

properties to surreptitiously capture and to disclose their Users' Private Information.[21] Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.[22]

B. Defendants Disclosed Patient Healthcare Information, Including Patient Status, in Violation of the HIPAA Privacy Rule

82. Healthcare entities collecting and disclosing Users' Private Information face significant legal exposure under HIPAA, which applies specifically to healthcare providers, health insurance providers and healthcare data clearinghouses. [23]

83. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information ("IIHI") that is held or transmitted. [24] This is information that can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

---

[21] The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment. Todd Feathers, *Meta Faces Mounting Questions from Congress on Health Data Privacy As Hospitals Remove Facebook Tracker*, https://themarkup.org/pixel-hunt/2022/09/19/meta-faces-mounting-questions-from-congress-on-health-data-privacy-as-hospitals-remove-facebook-tracker (last visited May 22, 2024).

[22] Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta's alleged patient data mining,* FIERCE HEALTHCARE (November 4, 2022), https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook.

[23] *Health Information Privacy* (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[24] The HIPAA Privacy Rule protects all electronically protected health information a covered entity like Defendants "created, received, maintained, or transmitted" in electronic form. *See* 45 C.F.R. § 160.103.

84. Plaintiff's IIHI captured by the Pixel and sent to Meta included their unique personal identifiers such as their Facebook ID, IP address, device identifiers and browser "fingerprints."

85. Defendants further violated the HIPAA Privacy Rule, among other statutory and common laws, because Plaintiff's PHI including their specific medical conditions (such as [redacted] was disclosed to Meta by the Pixel and other third-party trackers embedded by Defendants on its Web Properties.

86. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.[25] Thus, by purposely disclosing Plaintiff's activities on the Web Properties and the specialties and locations of Plaintiff's treating and other selected physicians to Meta, Defendants further violated the HIPAA Privacy Rule.

87. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

88. Defendants unlawfully revealed Plaintiff's and Class Members' patient status to Facebook and likely other unauthorized third parties in violation of HIPAA when the Meta Pixel captured and disclosed Plaintiff's and Class Members' activity on patient-dedicated webpages of the Web Properties.

[25] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited May 21, 2024).

C. HIPAA's Protections Do Not Exclude Internet Marketing

89. As the OCR reminded entities regulated under HIPAA (like Defendants) in its recently issued Use *of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* bulletin:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[26]

90. OCR makes it clear that information that is routinely collected by vendors on public-facing websites may be PHI, including unique identifiers such as IP addresses, device IDs, or email addresses.[27]

91. HHS has also confirmed that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the

[26] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*, note 20 (emphasis added) (last visited May 21, 2024).

[27] *See id.*; *see also* Mason Fitch, *HHS Bulletin Raises HIPAA Risks for Online Tracking Vendors*, LAW360 (December 13, 2022), https://www.law360.com/articles/1557792/hhs-bulletin-raises-hipaa-risks-for-online-tracking-vendors?copied=1.

> individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care.[28]

92. Further, HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal, i.e. to "unauthenticated" webpages:

> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … [and ***pages] that address[] specific symptoms or health conditions***, such as pregnancy or miscarriage, ***or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances***. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

93. **The HHS bulletin reminds covered entities, like Defendant, of its long-standing duty to safeguard PHI**, explicitly noting that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," and proceeding to explain how online tracking technologies violate the same HIPAA privacy rules that have existed for decades.[29]

94. Disclosures of PHI for online marketing or sales purposes require patient authorization under HIPAA, which Defendants did not obtain here. *See* 45 CFR § 164.508(a)(3) ("a covered entity must obtain an authorization for any use or disclosure of protected health information for marketing, except if the communication is in the form of: (A) a face-to-face

[28] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*, note 20 (emphasis added).

[29] *Id.* (emphasis added).

communication made by a covered entity to an individual; or (B) a promotional gift of nominal value provided by the covered entity."); 45 CFR § 164.508(a)(4) ("a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart [and] [s]uch authorization must state that the disclosure will result in remuneration to the covered entity.").

95. As a result, a healthcare provider like Defendants may not disclose PHI to a tracking technology vendor, like Meta, unless they have properly notified their Website Users and entered into a business associate agreement with the vendor in question.

96. Despite this clear guidance, Defendants elected to disclose Plaintiff's and Class Members' PHI without their consent and without a business associate agreement with Meta anyway.

D. The Industry was Warned of Third-Party Tracking Tools Resulting in HIPAA Violations, but Defendants Elected to Continue Their Illicit Sharing Anyway.

97. Recognizing the distinct privacy dangers third-party tracking tools present, the Federal Trade Commission ("**FTC**") joined HHS in warning HIPAA-covered entities and non-HIPAA covered entities alike that unauthorized disclosure of sensitive health information is through online tracking technology must be prevented.[30]

98. According to the FTC, "health information" is "anything that conveys information – or enables an inference – about a consumer's health" and provides an example that location-data

[30] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FEDERAL TRADE COMMISSION (Jul. 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

alone (such as "repeated trips to a cancer treatment facility") "may convey highly sensitive information about a consumer's health."[31]

99. The FTC and HHS explicitly warned the industry and healthcare providers like Defendants that transmitting "health information" to Google and Facebook via third-party tracking tools is an unfair business practice:

> "When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."[32]

100. Indeed, this decree by the FTC responds to real consumer concern for the privacy of their medical information. A recent national study from CVS Health revealed that nearly 90% of people found data security and privacy (e.g., keeping private health information confidential) among the most important factors concerning health care.[33]

101. This underscores the severity of Defendants' use of tracking technology like the "Meta/Facebook pixel" that, as the FTC alerts, "gather[s] identifiable information about users, []

[31] Elisa Jillson, *A baker's dozen takeaways from FTC cases*, FEDERAL TRADE COMMISSION (Jul. 25, 2023), https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases.

[32] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, supra,* note 30.

[33] *The 2021 Health Care Insights Study*, CVS HEALTH (2021), https://www.cvshealth.com/content/dam/enterprise/cvs-enterprise/pdfs/2021/cvs-health-health-care-insights-study-2021-report-executive-summary.pdf (last visited May 21, 2024).

without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app."[34]

102. The FTC and HHS warning to the healthcare industry highlights the "[r]ecent research,[35] news reports,[36] FTC enforcement actions,[37] and [] OCR bulletin[38]" concerning the privacy risks resulting from the use of tracking technologies like Meta Pixel.

103. The industry wide warning delineates that these privacy risks are the very privacy violations that HIPAA Privacy Rules are designed to protect against:

> "If you are a covered entity or business associate ("regulated entities") under HIPAA, you **must** comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.
>
> The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third

[34] *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies, supra,* note 30.

[35] Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, ASSOCIATION FOR COMPUTING MACHINERY (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[36] *See, e.g.*, Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[37] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (Jul. 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[38] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, supra*, note 20 (updated March 18, 2024) (last visited May 21, 2024).

> parties (e.g., tracking technology vendors) includes PHI. **HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules**. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies."[39]

104. As HIPAA-regulated entities, Defendants were required to comply with HIPAA Privacy Rules and heed this warning. However, Defendants chose to continue siphoning Plaintiff's and Class Members' PHI, in knowing violation of HIPAA and the wealth of regulatory guidance, and in conscious disregard of clear federal warnings and consumer concern.

105. Meta also chose to continue Pixel tracking practices on Defendants' Web Properties despite these clear warnings, prioritizing targeted advertising generated revenues over federal guidance prohibiting the use tracking technologies in a manner that would result in impermissible disclosures of PHI.

E. Defendants Transmitted A Broad Spectrum of Plaintiff's & Class Members' Identifiable Health Information to Meta via the Meta Tracking Tools.

106. Every website is comprised of "Markup" and "Source Code." Markup consists of the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendants' Web Properties.

107. Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

[39] *Model Letter: Use of Online Tracking Technologies*, FEDERAL TRADE COMMISSION (Jul. 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf .

Source Code is designed to be readable by humans and formatted in a way that developers and other users can understand.

108. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions including the ability to command a website user's browser to send data transmissions to third parties like Facebook, via the Meta Pixel. [40]

109. Defendants' Pixel, embedded in its JavaScript Source Code on the Web Properties, manipulates a User's browser by secretly instructing it to duplicate a User's communications (HTTP Requests) and sending those communications to Facebook.

110. This occurs because the Pixel is programmed to automatically track and transmit Users' communications, and this occurs contemporaneously, invisibly, and without the Users' knowledge.

111. Defendants' Source Code essentially commands a patient's browser to re-direct their actions on the Web Properties (characterized as "Event Data" by the Pixel), which contain PHI, through the HTTPS protocol to Meta at a Meta "endpoint," i.e., a URL at a domain controlled by Meta that exists for the purpose of acquiring such information.

112. The information Defendants send to Meta from its use of the Meta Pixel and other tracking tools includes, but is not limited to, the following:

a. The exact search terms entered by a User on the Website, including searches for the User's medical symptoms and conditions, specific medical providers and their specialty, and treatments sought;

b. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

c. the communications a User exchanges through Defendants' Web Properties by clicking and viewing webpages, including

[40] These Pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

> communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including whether they are made while a User is still logged in to the Patient Portal or around the same time that the User has scheduled an appointment, called the medical provider, or logged in or out of the Patient Portal;

d. locations of healthcare facilities and healthcare providers.

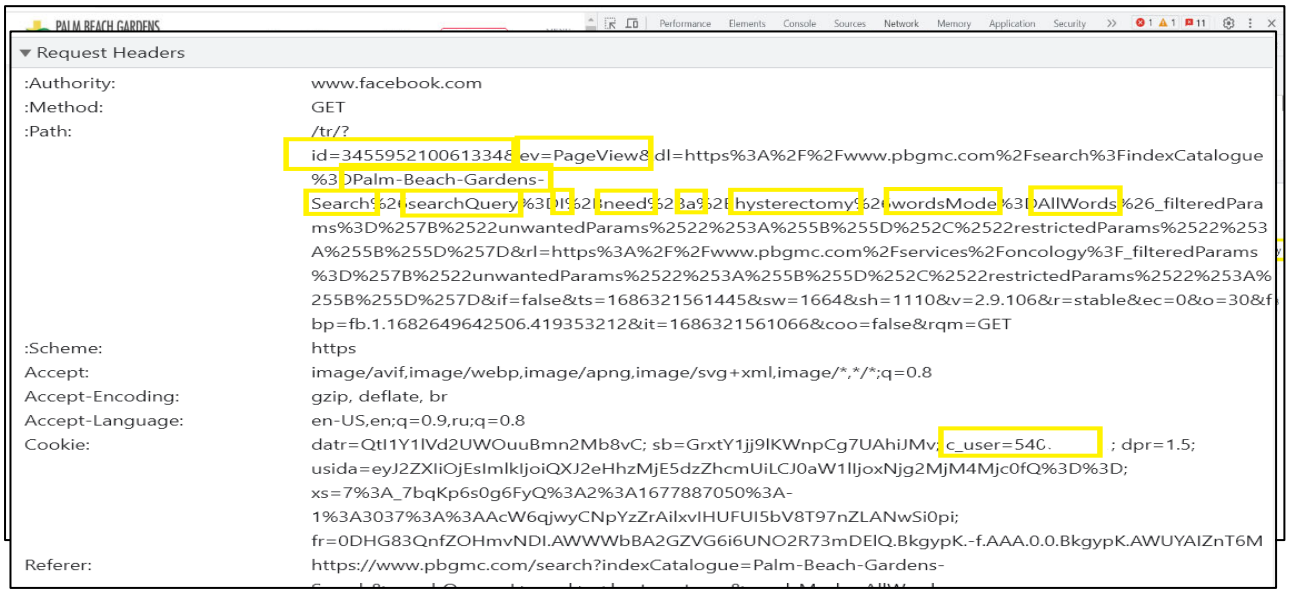
113. Thus, Defendants are, in essence, handing patients a tapped device and once one of their webpages is loaded into the User's browser, the software-based wiretap is quietly waiting for private communications on the webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to unauthorized third parties such as Facebook.

114. For example, when a patient visits the Web Properties and enters "I need a hysterectomy" into the search bar, their browser automatically sends an HTTP request to Defendants' web server. The web server automatically returns an HTTP response, which loads the Markup for that particular webpage.

115. The patient visiting this particular web page only sees the Markup, not Defendants' source code or underlying HTTP Requests and Responses.

116. In reality, Defendants' Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that a User was looking for treatment for their gynecological conditions associated with hysterectomy as a treatment—along with the User's unique personal identifiers.

Figures 1 and 2. An HTTP single communication session sent from the device to Facebook that reveals the User's exact search terms ("I need a hysterectomy") along with the User's unique Facebook personal identifier (the c_user field)[41]



117. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions and can command a website visitor's browser to send data transmissions to third parties via Pixels or web bugs,[42] effectively open a spying window through which the webpage can funnel the visitor's data, actions, and communications to third parties.

118. Looking to the previous example, Defendants' Source Code manipulates the patient's browser by secretly instructing it to duplicate the patient's communications (HTTP Requests) and sending those communications to Facebook.

119. This occurs because the Pixel embedded in Defendants' Source Code is programmed to automatically track and transmit a patient's communications, and this occurs contemporaneously, invisibly, and without the patient's knowledge.

---

[41] Images depicted in Figures 1 and 2 were taken from https://www.pbgmc.com/search?indexCatalogue=Palm-Beach-Gardens-Search&searchQuery=I+need+a+hysterectomy&wordsMode=AllWords.

[42] These Pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

120. Thus, without Users' consent, Defendants effectively use this Source Code to commandeer patients' computing devices, thereby re-directing their Private Information to unauthorized third parties.

121. The information that Defendants' Pixel sends to Facebook may include, among other things, patients' PII, PHI, and other confidential information.

122. Consequently, when Plaintiff and Class Members visit Defendants' Web Properties and communicate their Private Information, it is transmitted to Facebook, including, but not limited to: (i) patient status, (ii) health conditions, (iii) sought treatments or therapies, (iv) the specialty and location of personal, treating, and other physicians and providers sought together with any medical specialties, (v) appointments sought, (vi) selected locations or facilities for treatment, (vii) specific button/menu selections, (viii) sensitive demographic information such as sexual orientation, and (ix) exact words and phrases typed into the search bar.

F. Defendants' Pixel Tracking Practices Caused Plaintiff's and Class Members' Private Information to be Sent to Facebook.

123. Defendants utilize Facebook's Business Tools and intentionally installed the Pixel on their Web Properties to secretly track patients by recording their activity and experiences in violation of its common law, contractual, statutory, and regulatory duties and obligations.

124. Defendants' web pages contain a unique identifier which indicates that the Pixel is being used on a particular webpage.[43]

125. The Pixels allow Defendants to optimize the delivery of advertisements, measure cross-device conversions, create custom audiences, and decrease advertising and marketing costs.

[43] Upon information and belief, Defendants' Websites had more than one Meta Pixel installed on various web pages. These same Pixels were embedded across different websites for various hospitals and networks within Defendant Tenet's healthcare system.

126. However, Defendants' Web Properties do not rely on the Pixel to function.

127. While seeking and using Defendants' services as a medical provider, Plaintiff and Class Members communicated their Private Information to Defendants via their Web Properties.

128. Defendants did not disclose to Plaintiff and Class Members that their Private Information would be shared with Facebook as it was communicated to Defendants. Rather, Defendants represented the opposite. This prevents the provision of any informed consent by Plaintiff or Class Members to Defendants for the challenged conduct described herein.

129. Plaintiff and Class Members never consented, agreed, authorized, or otherwise permitted Defendants to disclose their Private Information to Facebook (or any other third party), nor did they intend for Facebook to be a party to their communications with Defendants.

130. Defendants do not employ any form or click system whereby Plaintiff and Class Members provide their affirmative consent to Defendants agreeing, authorizing, or otherwise permitting Defendants to disclose their Private Information to Facebook (or any other third party).

131. Defendants sent sensitive Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatment or therapies; (iv) terms and phrases entered into Defendants' search bar; (v) the specialty and location of personal, treating, and other physicians and providers sought together with any medical specialties; (vi) selected locations or facilities for treatment; and (vii) web pages viewed.

132. Importantly, the Private Information Defendants' Pixels sent to Facebook was sent alongside Plaintiff's and Class Members' personal identifiers, including patients' IP address and cookie values thereby allowing individual patients' communications with Defendants, and the

Private Information contained in those communications, to be linked to their unique Facebook accounts.

133. Through the Source Code deployed by Defendants, the cookies that they use to help Facebook identify patients include but are not necessarily limited to cookies named: "c_user," "datr," "fr," and "fbp."[44]

134. The "*c_user*" cookie or FID is a type of third-party cookie assigned to each person who has a Facebook account, and it is composed of a unique and persistent set of numbers.

135. A User's FID is linked to their Facebook profile, which generally contains a wide range of demographics and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

136. The "*datr*" cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users. Facebook keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Facebook.

[44] Defendants' Websites track and transmit data via first-party and third-party cookies. C_user, datr, and fr cookies are third-party cookies. The fbp cookie is a Facebook identifier that is set by Facebook source code and associated with Defendants' use of the Facebook Pixel. The fbp cookie emanates from Defendants' Websites as a putative first-party cookie, but is transmitted to Facebook through cookie syncing technology that hacks around the same-origin policy.

137. The "*fr*" cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[45]

G. *Defendants' Pixel Disseminates Patient Information Via Their Web Properties.*

138. As described herein, Defendants' Meta Pixel (and other third-party trackers) sent sensitive Private Information to Facebook, including but not limited to Plaintiff's and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatments or therapies; (iv) terms and phrases entered into Defendants' search bar; (v) searches for doctors; (vi) locations of facilities for treatment; and (vii) web pages viewed.

139. By way of example, if a patient uses https://www.pbgmc.com/ to look for medical treatments, they may select "Oncology" under the "Services" tab, which takes them to the list of services offered by Defendants to Users in need of cancer treatments. On those pages the User can further narrow their search results by services offered by Defendants.

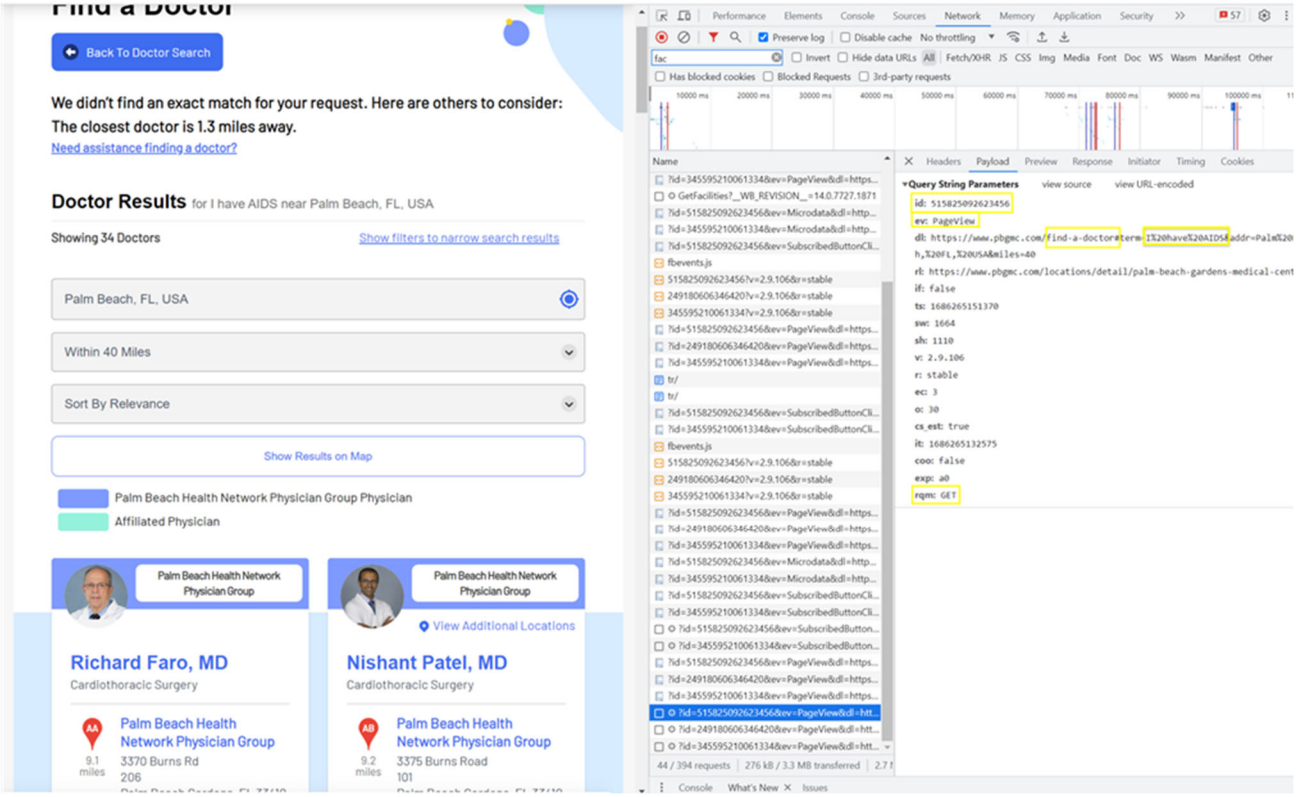
140. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries, without alerting the User, and the images below confirm that the communications Defendants send to Facebook contain the User's Private Information and personal identifiers, including but not limited to their IP address, Facebook ID, and datr and fr cookies, along with the search filters the User selected.

141. For example, an AIDS patient can search for various care options and service providers.

[45] *See* Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

142. From the moment the patient begins the search "I have AIDS", their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers, as evidenced by Figures 3 and 4 below.

Figure 3. Defendants' transmission to Facebook of User's search parameters showing treatment sought ("I have AIDS").



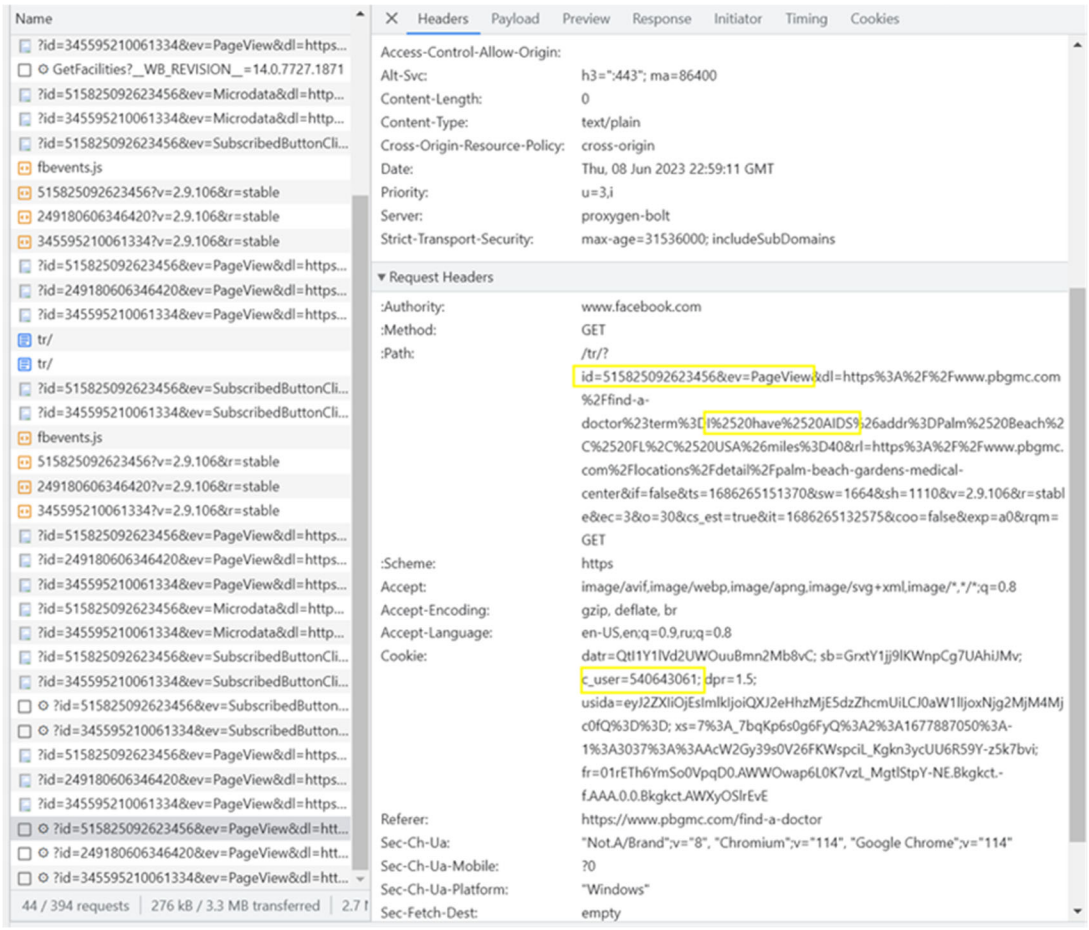
143. The first line of highlighted text, "id: 515825092623456," refers to Defendants' Pixel ID for this particular Webpage and confirms that Defendants have downloaded the Pixel into their Source Code on this particular Webpage.

144. In the second line of text, "ev:" is an abbreviation for event, and "PageView" is the type of event. Here, this event means that Defendants' Pixel is notifying them that you landed on the webpage.

145. The remaining lines of text identify the User as a patient: (i) seeking medical care from Defendants via www.pbgmc.com; (ii) who has AIDS; and (iii) who is searching for a doctor.

146. The last line of highlighted text ("GET"), demonstrates that Defendants' Pixel sent the User's communications, and the Private Information contained therein, alongside the User's personal identifiers, including Facebook ID and other cookies. This is further evidenced by the image below, which was collected during the same browsing session as the previous image.

Figure 4. Defendants' transmission to Facebook of User's search parameters showing the search term ("I have AIDS") and the User's unique Facebook ID.

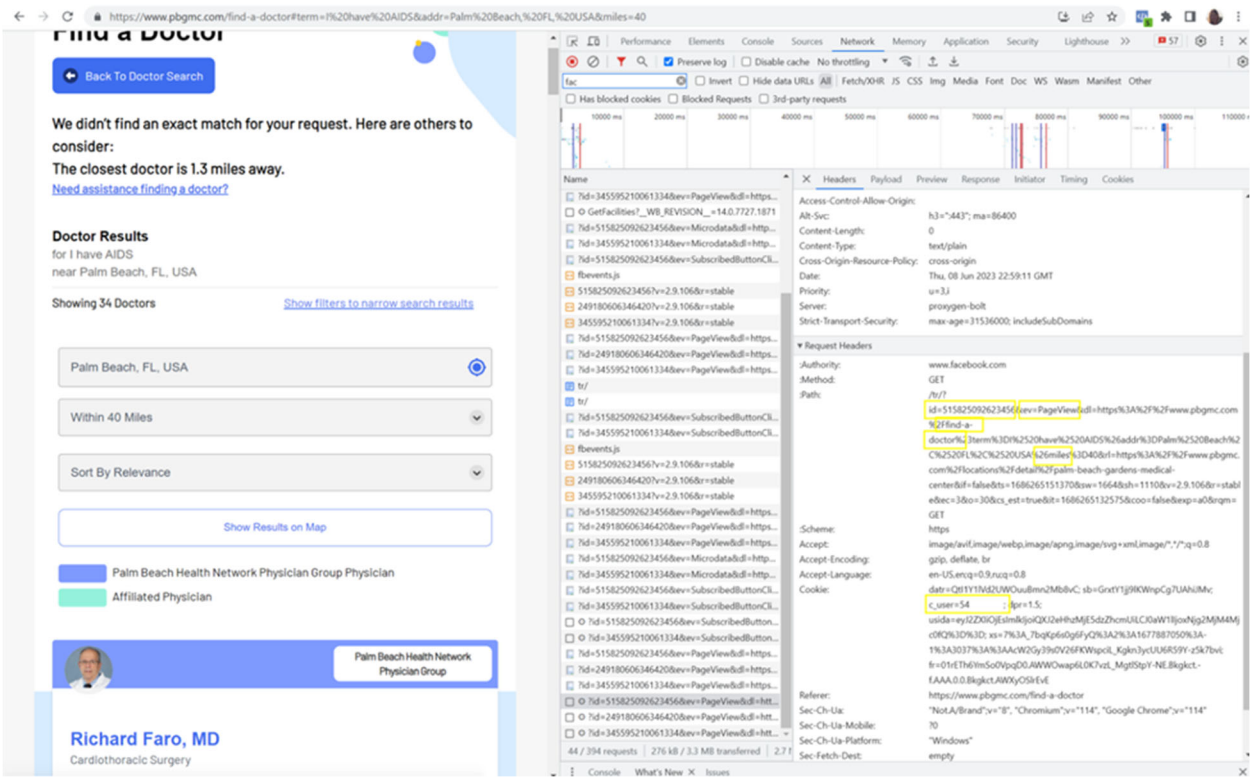


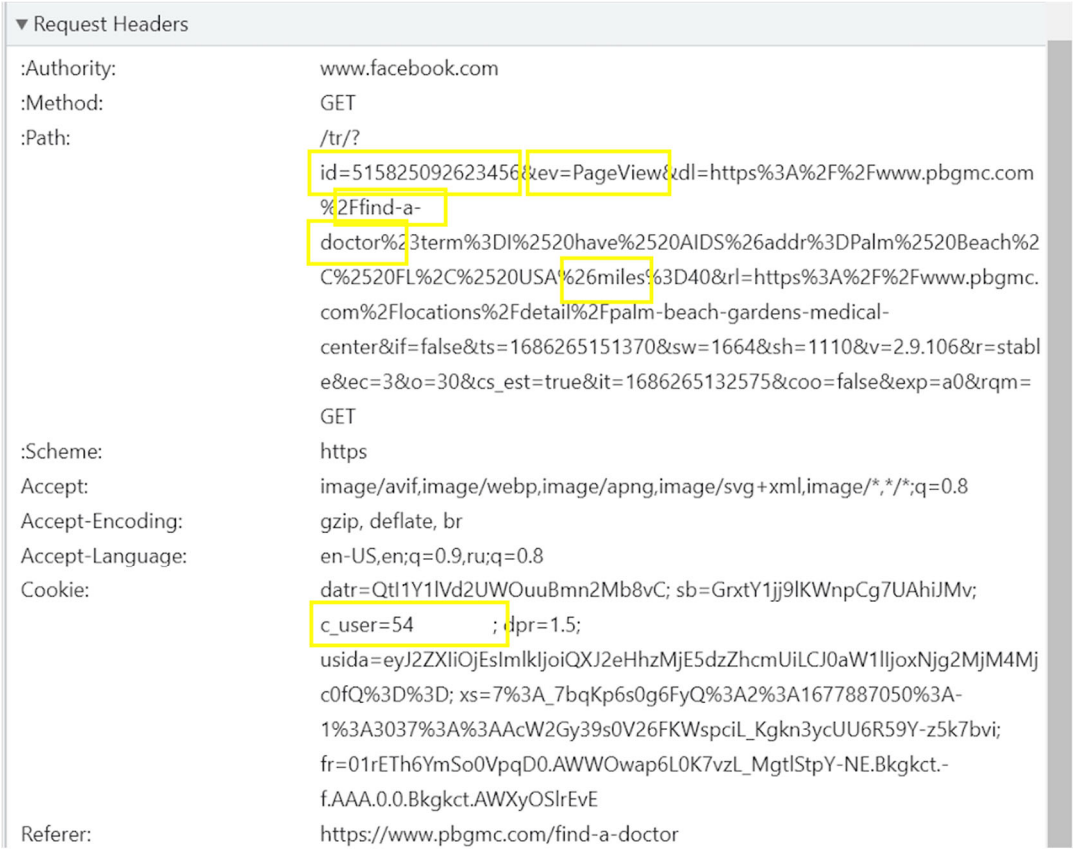
147. As mentioned above, if the patient selects other AIDS services, those search parameters are also automatically transmitted to Facebook by Defendants' Pixels, along with the patient's personal identifiers.

148. Additionally, a patient can use Defendants' Websites such as https://www.pbgmc.com/ to search for a provider based on their name, specialty, or distance from the patient's location.

149. These search terms are also transmitted via the Facebook Pixel:

Figures 5 and 6. Defendants' transmission to Facebook of User's search parameters showing search terms ("Find a Doctor" and "26 miles") and the User's c_user information from search results via Defendants' search bar.





▼ Request Headers

:Authority:	www.facebook.com
:Method:	GET
:Path:	/tr/? id=515825092623456&ev=PageView&dl=https%3A%2F%2Fwww.pbgmc.com%2Ffind-a-doctor%23term%3DI%2520have%2520AIDS%26addr%3DPalm%2520Beach%2C%2520FL%2C%2520USA%26miles%3D40&rl=https%3A%2F%2Fwww.pbgmc.com%2Flocations%2Fdetail%2Fpalm-beach-gardens-medical-center&if=false&ts=1686265151370&sw=1664&sh=1110&v=2.9.106&r=stable&ec=3&o=30&cs_est=true&it=1686265132575&coo=false&exp=a0&rqm=GET
:Scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9,ru;q=0.8

Cookie:	datr=QtI1Y1lVd2UWOuuBmn2Mb8vC; sb=GrxtY1jj9lKWnpCg7UAhiJMv;
	c_user=54 ; dpr=1.5;
	usida=eyJ2ZXIiOjEsImlkIjoiQXJ2eHhzMjE5dzZhcmUiLCJ0aW1lIjoxNjg2MjM4Mjc0fQ%3D%3D; xs=7%3A_7bqKp6s0g6FyQ%3A2%3A1677887050%3A-1%3A3037%3A%3AAcW2Gy39s0V26FKWspciL_Kgkn3ycUU6R59Y-z5k7bvi;
	fr=01rETh6YmSo0VpqD0.AWWOwap6L0K7vzL_MgtlStpY-NE.Bkgkct.-f.AAA.0.0.Bkgkct.AWXyOSlrEvE

Referer:	https://www.pbgmc.com/find-a-doctor

150. This information is automatically sent from the User's device to Facebook, and it reveals the User's FID (c_user field) along with each search filter the User selected.

151. Finally, Defendants' Websites also share with Facebook each time a User wants to register for the Portal or the fact that a patient is trying to access the Portal.

152. A User who accesses Defendants' Websites while logged into Facebook will transmit the c_user cookie to Facebook, which contains that User's unencrypted Facebook ID, and other personal cookie values including the datr and fr cookies.

153. When a User's browser has recently logged out of their Facebook account, Facebook compels the User's browser to send a smaller set of cookies:[46]

Figure 7

fr	00Zp...	.facebook.com
wd	1156...	.facebook.com
sb	qqAz...	.facebook.com
datr	Malz...	.facebook.com

H. Defendants Violate Their Promises to Users and Patients to Protect Their Confidentiality.

154. Hospitals, including Defendants, possess the capability to activate tracking Pixels on their websites to monitor and analyze every activity of their visitors. When such Pixel technology is enabled, these hospitals, by default, agree with Facebook's terms (by using Meta's Business Tools the health care provider or covered entity "represent[s] and warrant[s] that [it has] provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage"[47]) which necessitate an assertion from the hospitals: that they have secured explicit consent from their patients, including Plaintiff, to relay their tracking data, communications, diagnosis, and other pertinent medical details to Facebook.

155. Defendants do not have the legal right to use or share Plaintiff's and Class Members' data, as this information is protected by the HIPAA Privacy Rule. The Privacy Rule

[46] The screenshot below serves as an example and demonstrates the types of data transmitted during an HTTP single communication session. Not pictured here and in the preceding image is the _fbp cookie, which is transmitted as a first-party cookie.

[47] *Meta, Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors.

does not permit the use and disclosure of Private Information to Facebook for use in targeted advertising.[48]

156. Beyond Defendants' legal obligations to protect the confidentiality of individuals' Private Information, Defendants' privacy policies and online representations affirmatively and unequivocally state that any personal information provided to Defendants will remain secure and protected.[49]

157. Further, Defendants represent to Users that they will only disclose Private Information provided to them under certain circumstances, ***none of which apply here***.[50] Defendants' privacy policies do ***not*** permit Defendants to use and disclose Plaintiff's and Class Members' Private Information for marketing purposes.

158. In fact, Defendants acknowledge in their (identical) Notices of Privacy Practices that they must obtain Users' "written authorization"[51] to use their PHI to send them any marketing materials.

159. Moreover, Defendants represent that they will not disclose Users' PHI without their authorization "in exchange for direct or indirect payment except in limited circumstances permitted by law. These circumstances include public health activities; research; treatment of the individual; sale, transfer, merger or consolidation of the Facility; services provided by a business associate, pursuant to a business associate agreement; providing an individual with a copy of their

[48] *See* 45 C.F.R. § 164.502.

[49] *Notice of Privacy Practices*, PALM BEACH HEALTH NETWORK, https://www.palmbeachhealthnetwork.com/privacy-policy (last visited May 21, 2024).

[50] *Id*.

[51] *Id.*

PHI; and other purposes deemed necessary and appropriate by the U.S. Department of Health and Human Services (HHS)."[52]

160. Upon information and belief, Defendants do not have a business associate agreement with Facebook, and none of the "limited circumstances" listed above apply here.

161. Further, in their Privacy Policy Defendants represent:

> "***We do not sell personal information that we have collected from consumers to any third parties***."
>
> "We may collect certain information by automated means. This information includes cookies, sensors, geo location, pixel tags, IP addresses, mobile device information and other similar technology. ***This information does not identify you, but is statistical data that provides generic information about your use of the Sites.***"
>
> "We take reasonable, industry standard precautions to keep the Sites and their systems secure and to prevent personal information from being made available to unauthorized persons or entities."[53]

162. Finally, in their Notices of Privacy Practices, Defendants acknowledge that they are "required by law to protect the privacy of [Users'] medical information" and "to notify [them] if there is a breach or impermissible access, use or disclosure of [their] medical information."[54] Plaintiff relied on these privacy representations in using Defendant PBGMC's Web Properties.

163. Defendants failed to issue a notice that Plaintiff and Class Members' Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendants

---

[52] *Id*.

[53] *Privacy Policy*, *supra*, note 6.

[54] *Notice of Privacy Practices*, https://www.palmbeachhealthnetwork.com/notice-of-privacy-practices (last visited May 21, 2024).

never disclosed to Plaintiff or Class Members that they shared their sensitive and confidential communications, data, and Private Information with Facebook and other third parties.[55]

164. Defendants have unequivocally failed to adhere to a single promise vis-à-vis their duty to safeguard Private Information of their Users. Defendants have made these privacy policies and commitments available on their Websites. Defendants included these privacy policies and commitments to maintain the confidentiality of their Users' sensitive information as terms of their contracts with those Users, including contracts entered with Plaintiff and Class Members.

165. In these contract terms and other representations to Plaintiff and Class Members and the public, Defendants promised to take specific measures to protect Plaintiff's and Class Members' Private Information, consistent with industry standards and federal and state law. However, they failed to do so.

166. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.[56]

---

[55] In contrast to Defendants, several medical providers which have installed the Meta Pixel on their Web Properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited May 21, 2024); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

[56] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUM. SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited May 21, 2024).

167. Facebook further also claims that "providers [...] will not send [patient information] to Meta because it violates Meta's contracts for them to be doing that."[57]

168. Despite a lack of disclosure, Defendants enabled third parties to "listen in" on patients' confidential communications in knowing violation of HIPAA and to intercept and use for advertising purposes the very information it promised to keep private, in order to bolster their profits.

I. Plaintiff and Class Members Reasonably Believed That Their Confidential Medical Information Would Not Be Shared with Third Parties.

169. Plaintiff and Class Members were aware of Defendants' duty of confidentiality when they sought medical services from Defendants.

170. Indeed, at all times when Plaintiff and Class Members provided their Private Information to Defendants, they each had a reasonable expectation that the information would remain confidential and that Defendants would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

171. Personal data privacy and obtaining consent to share Private Information are material to Plaintiff and Class Members.

172. Plaintiff and Class Members relied to their detriment on Defendants' uniform representations and omissions regarding protection privacy, limited uses, and lack of sharing of their Private Information.

173. Specifically, Plaintiff and Class Members relied on Defendants' promises that they "do not sell personal information [] collected from consumers to any third parties," that any

[57] *Id.* at 7:20-8:11.

information collected would not "identify" them and would reflect "generic information about [their] use of the Sites."[58]

174. Plaintiff and Class Members believed and relied upon Defendants' representation that they "take reasonable, industry standard precautions to keep the Sites and their systems secure and to prevent personal information from being made available to unauthorized persons or entities."[59]

175. Based on Defendants' representations, Plaintiff and Class Members did not think that every click, key stroke, search term, and more would be siphoned out to third parties like Facebook for targeted advertising pertaining to their private, sensitive medical conditions.

176. Now that their sensitive personal and medical information is in possession of third parties, Plaintiff and Class Members face a constant threat of continued harm – including bombardment of targeted advertisements based on the unauthorized disclosure of their personal data. Collection and sharing of such sensitive information without consent or notice poses a great threat to individuals by subjecting them to the never-ending threat of identity theft, fraud, phishing scams, and harassment.

J. *Plaintiff and Class Members Have No Way of Determining Widespread Usage of Invisible Pixels.*

177. Plaintiff and Class Members had no idea that Defendants collect and utilize their Private Information, including sensitive medical information, when they engage with Defendants' Websites which have Meta Pixels secretively incorporated in the background.

178. Patients and Users of Defendants' Websites did not receive any alerts during their uses of Defendants' Web Properties stating that Defendants track and share sensitive medical data

[58] *Privacy Policy, supra,* note 6.

[59] *Id.*

with Facebook, allowing Facebook and other third parties to subsequently target all users of Defendants' Websites for marketing purposes.

179. Plaintiff and Class Members trusted Defendants when inputting sensitive and valuable Private Information in their Web Properties. Had Defendants disclosed to Plaintiff and Class Members that every click, every search, and every input of sensitive information was being tracked, recorded, collected, and ***disclosed*** to third parties, Plaintiff and Class Members would not have trusted Defendants' Websites to input such sensitive information.

180. Defendants knew or should have known that Plaintiff and Class Members would reasonably rely on and trust Defendants' promises regarding the tracking privacy and uses of their Private Information. Furthermore, any person visiting a health website has a reasonable understanding that medical providers must adhere to strict confidentiality protocols and are bound not to share any medical information without their consent.

181. By collecting and sharing Users' Private Information with Facebook and other unauthorized third parties, Defendants caused harm to Plaintiff, Class Members, and all affected individuals.

182. Furthermore, once Private Information is shared with Facebook, such information may not be effectively removed, even though it includes personal and private information.

183. Plaintiff fell victim to Defendants' unlawful collection and sharing of their sensitive medical information using the Meta Pixel tracking code on their Websites.

K. Defendants Knew Plaintiff's Private Information Included Sensitive Medical Information, Including Medical Records.

184. By virtue of how the Meta Pixel works, Defendants were aware that by incorporating the Meta Pixel onto their Websites, this would result in the disclosure and use of Plaintiff's and Class Members' Private Information, including sensitive medical information.

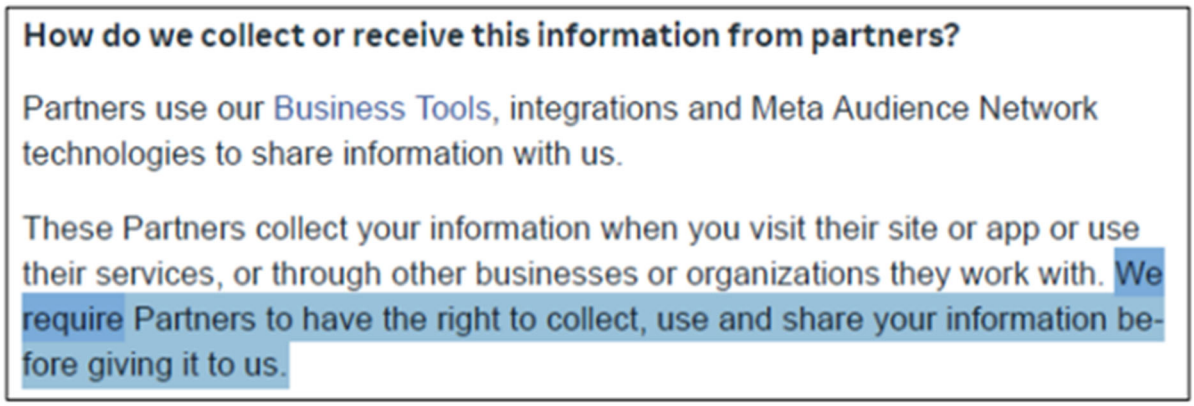
185. And Defendants were aware that Users' Private Information would be sent to Facebook when they researched specific medical conditions and/or treatments, looked up providers, made appointments with personal, treating, and other physicians, typed specific medical queries into the search bar, and otherwise interacted with Defendants' Web Properties.

186. Even though Meta actively wants to collect and track vast amount of data, including confidential medical data, publicly, to limit or possibly avoid liability, Meta notified its partners, including Defendants, they are to have the legal right to collect, use, and share user data before providing any data to Meta.[60] Defendants had been on notice of this Pixel-tracking ever since they activated such Pixel technology on their Websites.

> **Information from partners.**
> Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.
>
> Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.
>
> To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

[60] *See In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at *13-14 (N.D. Cal. Dec. 22, 2022).

187. Meta changed this provision again in July 2022, while still requiring partners to have the right to share patient information with Meta:[61]



How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

188. Though Meta's policies require health care providers to obtain consent from Users, Meta's *actual* intent is different: it wants to collect as much data as possible, including confidential medical data from Defendants' websites.

189. Despite the changes it made to this provision over time, Meta has never actually "required" health care providers or other covered entities, to have the right to "collect, use and share" patient information before redirecting it to Meta. It never verified such consent, nor imposed any enforcement mechanism whatsoever, to ensure that its "partners" had the right to share the data. If it had done so, Meta would have lost all access to the valuable medical data – as no hospital would have consent to share such sensitive data. For that reason, and to limit its potential exposure to liability, Meta merely included a provision in its form contract creating an unenforced "honor system," which requires hospitals like Defendants to "represent[s] and warrant[s] that [they have]

[61] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors.

provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage":[62]

> 3. Special Provisions Concerning the Use of Certain Business Tools
>
> a. This section applies to your use of Business Tools to enable Meta to store and access cookies or other information on an end user's device.
> b. You (or partners acting on your behalf) may not place pixels associated with your Business Manager or ad account on websites that you do not own without our written permission.
> c. You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage that includes, at a minimum:
>
> i. For websites, a clear and prominent notice on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Meta, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites and elsewhere on the Internet and use that information to provide measurement services, target and deliver ads, (b) how users can opt-out of the collection and use of information for ad targeting, and (c) where a user can access a mechanism for exercising such choice (e.g., providing links to: http://www.aboutads.info/choices and http://www.youronlinechoices.eu/).
> ii. For apps, a clear and prominent link that is easily accessible inside your app settings or any privacy policy and from within any store or website where your app is distributed that links to a clear explanation (a) that third parties, including Meta, may collect or receive information from your app and other apps and use that information to provide measurement services, target and deliver ads, and (b) how and where users can opt-out of the collection and use of information for ad targeting.
>
> d. In jurisdictions that require informed consent for storing and accessing cookies or other information on an end user's device (such as but not limited to the European Union), you must ensure, in a verifiable manner, that an end user provides all necessary consents before you use Meta Business Tools to enable the storage of and access to Meta cookies or other information on the end user's device. (For suggestions on implementing consent mechanisms, visit our Cookie Consent Resource.)

190. Instead of taking any steps to verify consent, notify the affected patients, or enforce its purported requirements for notice and consent, Meta makes the Pixel available to any advertisers who uses Meta's automated tools to create and deploy the Pixel. This process does not include any effort by Meta to require its Partners to have lawful rights to use the Pixel. Meta does nothing to determine whether an advertiser is placing the Pixel on a website that contains health information and through which Meta will acquire health information.

191. In response to congressional member's warnings concerning the risks that Pixel tracking poses to user health data,[63] Meta admitted that it has the ability to suspend or terminate a developer from using their Business Tools such as the Pixel. Meta has the capability to prevent the

[62] *Meta Business Tools Terms*, Facebook, https://m.facebook.com/legal/businesstech (last accessed May 21, 2024).

[63] Mark R. Warner, *Warner Expresses Concern Over Meta's Collection of Sensitive Health Information,* MARK. R. WARNER. U.S. SEN. FOR VIRGINIA (Oct. 20, 2022), https://www.warner.senate.gov/public/index.cfm/2022/10/warner-expresses-concern-over-meta-s-collection-of-sensitive-health-information.

unauthorized targeting advertising practices that utilize Defendants' patients' medical data, but chooses not to.

192. Meta has the means and technologically robust systems to utilize filters to require web developers to have the right to share health information with Meta, or offer patients/Users to *opt in/accept* tracking on various hospital website and alternatively to opt out/decline tracking on various hospital websites. Yet, Meta uses no such tools to (a) ensure that the affected Users are aware of Meta's extensive tracking; (b) ensure that it has the consent from the affected Users, (c) allow Users to opt out of such extensive tracking. Instead, Meta doubled down on its tracking activities by implementing tools that bypass even most sophisticated Users' implemented cookie blockers to ensure that it collects the data even when the most technologically advanced Users actively deploy tools to avoid being tracked by Meta.

193. Meta was (and likely still is) actively grouping the collected confidential medical data, and placing each individual into separate categories like health causes (i.e. lung cancer awareness, world diabetes day, chemotherapy), sexual orientation categories (i.e. same sex marriage, LGBT culture), and other categories, to target these specific individuals based on their health conditions, sexual preferences, and other categories such as race/religion etc.

194. Meta even allowed the advertisers to then target the specific affected individuals – such as Plaintiff here – the individuals with lung cancer and heart problems. Until recently, a pharmaceutical company or other advertisers could specifically isolate Plaintiff and other individuals with the same health conditions and bombard them with targeted ads based on their medical issues. Meta changed those settings only recently – highly likely in response to lawsuits and complaints it continued to receive from the affected patients.

195. Meta knowingly took data it knew has been obtain without consent anyway, unsupported with technology that easily could have equipped partners to comply, and looked the other way. Meta's tools and filters are not effective, not fully implemented, and call into question Meta's true intent. Meta's actual intent to harvest sensitive health data for targeted advertising is ongoing.[64]

196. Indeed, Meta partners with healthcare marketers, and urges health care providers and other covered entities to use the Pixel and other Meta tools to target ads to patients.[65]

197. Meta's unenforced directive and empty suggestion for Defendants to have the right to collect the data before sharing it with them does not vitiate Meta's intent: to harvest as much data, including sensitive medical information like that encompassed within Users' Private Information, to amass targeted advertising profiles for profit.

198. Defendants had the explicit option to disable the Pixel technology on their Web Properties, but chose not to exercise this option, thereby continuing to share data with Facebook despite the availability of preventive measures and industry wide warnings that it was violating HIPAA.

199. Defendants, in direct contravention Meta's unenforced suggestions to refrain from sending any information they did not have the legal right to send, the industry wide warnings, and more importantly, despite Defendants' promises to keep all health-related data about patients

[64] *See also Doe v. Meta Platforms, Inc*., No. 22-CV-03580-WHO, 2023 WL 5837443, at *3 (N.D. Cal. Sept. 7, 2023) (What Meta's true intent is, what steps it actually took to prevent receipt of health information, the efficacy of its filtering tools, and the technological feasibility of implementing other measures to prevent the transfer of health information, all turn on disputed questions of fact that need development on a full evidentiary record.")

[65] Meta, *Get held growing your healthcare business,* META, https://www.facebook.com/business/industries/consumer-goods/healthcare.

confidential, continued to employ Pixel tracking on their Websites, thereby sharing sensitive patient data without proper authorization or consent.

L. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their Private Information, Especially with Respect to Sensitive Medical Information.

200. Plaintiff and Class Members have a reasonable expectation of privacy in their Private Information, including personal information and sensitive medical information.

201. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. *See* 45 C.F.R. § 164. HIPAA also requires that covered entities implement appropriate safeguards to protect this information. *See* 45 C.F.R. § 164.530(c)(1).

202. This federal legal framework applies to health care providers, including Defendant.

203. Given the application of HIPAA to Defendants, Plaintiff and Class Members had a reasonable expectation of privacy over their PHI.

204. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the collection and unauthorized disclosure of sensitive medical information from millions of individuals, as Defendants have done here, violates expectations of privacy that have been established as general societal norms.

205. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

206. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites

should be required to provide consumers with a complete list of the data that has been collected about them.[66] Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[67]

207. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.[68]

208. Medical data is particularly even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are intended targets of cyber-criminals.[69]

209. Patients using Defendants' Web Properties must be able to trust that the information they input including their physicians, their health conditions and courses of treatment will be protected. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with particular medical conditions such as HIV or AIDS

---

[66] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[67] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[68] Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[69] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

that can and do subject them to regular discrimination. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.[70]

210. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[71] The article continues, "[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee — as yet — the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[72]

211. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated

[70] Bebe J. Anderson, JD, *HIV Stigma and Discrimination Persist, Even in Health Care*, AMA J. ETHICS (December 2009), https://journalofethics.ama-assn.org/article/hiv-stigma-and-discrimination-persist-even-health-care/2009-12.

[71] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, MIT PRESS READER (January 14, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

[72] *Id.*

in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.[73]

212. Defendants surreptitiously collected and used Plaintiff's and Class Members' Private Information, including highly sensitive medical information, through Meta Pixel in violation of Plaintiff's and Class Members' privacy interests.

213. Meta, in turn, perpetuated the surreptitious collection and misuse of Plaintiff's and Class Member' Private Information for targeted advertising and revenue generating purposes.

M. Defendants Were Enriched & Benefitted from the Use of the Pixel & other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.

214. Meta advertises its' Pixel as a piece of code "that can help you better understand the ***effectiveness of your advertising*** and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system ***decrease your costs***."[74]

215. Retargeting is a form of online marketing that targets Users with ads based on previous internet communications and interactions. Retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[75]

---

[73] *See* Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF Medical Center*, CLASS ACTION (Feb. 9, 2023), https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf.

[74] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited May 21, 2024).

[75] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited May 21, 2024).

216. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendants' Websites.

217. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken - all of which could be potential examples of health information."[76]

218. In exchange for disclosing the Private Information of their patients, Defendants are compensated by Facebook and likely other third parties in the form of enhanced advertising services and more cost-efficient marketing on their platform.

219. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many are not HIPAA-complaint or are only HIPAA-compliant if certain steps are taken.[77]

220. For example, Freshpaint a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant", and "If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[78]

221. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[79]

---

[76] *Id*.

[77] *See* PIWIK Pro, *The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited May 21, 2024).

[78] *Id*.

[79] *The complex world of healthcare retargeting, supra*, note 75.

222. Thus, utilizing the Pixels directly benefits Defendants by, among other things, reducing the cost of advertising and retargeting.

N. *Plaintiff's & Class Members' Private Information Has Substantial Value.*

223. Plaintiff's and Class Members' Private Information had value, and Defendants' disclosure and interception harmed Plaintiff and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

224. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

225. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[80] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[81] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

226. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to continue increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

227. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[82]

---

[80] *See The world's most valuable resource is no longer oil, but data*, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited May 21, 2024).

[81] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited May 21, 2024).

[82] *See 10 Apps for Seling Your Data for* Cash, https://wallethacks.com/apps-for-selling-your-data/ (last visited May 21, 2024).

228. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

229. In 2023, the Value Examiner published a report that focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[83]

230. In 2021, Trustwave Global Security published a report entitled *Hackers, breaches and the value of healthcare data*. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[84]

231. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "*How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.74[85]

---

[83] *See Valuing Healthcare Data*, https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited May 21, 2024).

[84] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (citing *The Value of Data*, https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited May 21, 2024).

[85] *See* https://time.com/4588104/medical-data-industry/ (last visited May 21, 2024).

232. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."75[86]

233. The dramatic difference in the price of healthcare data when compared to other forms of private information that is commonly sold is evidence of the value of PHI.

234. But these rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

235. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

TOLLING, CONCEALMENT & ESTOPPEL

236. The applicable statutes of limitation have been tolled as a result of Defendants' knowing and active concealment and denial of the facts alleged herein.

237. Defendants secretly incorporated the Meta Pixel into their Web Properties and patient portals, providing no indication to Users that their User Data, including their Private Information, would be disclosed to unauthorized third parties.

238. Defendants had exclusive knowledge that the Meta Pixel was incorporated on its Web Properties, yet failed to disclose that fact to Users, or inform them that by interacting with their websites Plaintiff's and Class Members' User Data, including Private Information, would be disclosed to third parties, including Facebook.

239. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct because the incorporation of Meta Pixels is highly technical and

[86] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited May 21, 2024).

there were no disclosures or other indications that would inform a reasonable consumer that Defendants were disclosing and allowing Facebook to intercept Users' Private Information.

240. The earliest Plaintiff and Class Members could have known about Defendants' conduct was shortly before the filing of this Complaint.

241. As alleged above, Defendants have a duty to disclose the nature and significance of their data disclosure practices but failed to do so. Defendants are therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ALLEGATIONS

242. **Class Definition:** Plaintiff brings this action on behalf of themself and on behalf of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure:

243. The **Nationwide Class** that Plaintiff seeks to represent is defined as:

> All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendants' Web Properties.

244. The **Florida Subclass** that Plaintiff seeks to represent is defined as:

> All individuals residing in the State of Florida whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendants' Web Properties.

245. The Nationwide Class and the Florida Class are referred to collectively as the "Classes."

246. **The following people are excluded from the Classes:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest and its current or former officers and directors; (3) persons who properly

execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

247. Plaintiff reserves the right under Federal Rule of Civil Procedure 23 to amend or modify the Classes to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues. Plaintiff reserves the right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of particular issues.

248. The elements of Federal Rule of Civil Procedure 23 are all satisfied.

249. **Numerosity:** The exact number of Class Members is not available to Plaintiff, but it is clear that individual joinder is impracticable. Millions of people have used Palm Beach Health Network, Palm Beach Gardens Medical Center, and Tenet Healthcare Corporation's services since at least 2015. Class Members can be identified through Defendants' records or by other means.

250. **Commonality:** Commonality requires that Class Members' claims depend upon a common contention such that determination of its truth or falsity will resolve an issue that is central to the validity of each claim in one stroke. Here, there is a common contention for all Class Members as to whether Defendants disclosed to third parties their Private Information without authorization or lawful authority.

251. **Typicality:** Plaintiff's claims are typical of the claims of other Class Members in that Plaintiff and Class Members sustained damages arising out of Defendants' uniform wrongful conduct and data sharing practices.

252. **Adequate Representation:** Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's claims are made in a representative capacity on

behalf of Class Members. Plaintiff has no interests antagonistic to the interests of the other Class Members. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of Class Members.

253. The declaratory and injunctive relief sought in this case includes, but is not limited to:

a. Entering a declaratory judgment against Defendants—declaring that Defendants' interception of Plaintiff's and Class Members' Private Information among themselves and other third parties is in violation of the law;

b. Entering an injunction against Defendants:

i. preventing Defendants from sharing Plaintiff's and Class Members' Private Information among themselves and other third parties;

ii. requiring Defendants to alert and/or otherwise notify all users of its websites and portals of what information is being collected, used, and shared;

iii. requiring Defendants to provide clear information regarding their practices concerning data collection from the users/patients of Defendants' Web Properties, as well as uses of such data;

iv. requiring Defendants to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

v. and requiring Defendants to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendants' Web Properties.

254. **Predominance:** There are many questions of law and fact common to the claims of Plaintiff and Class Members, and those questions predominate over any questions that may

affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

a. Whether Defendants' unauthorized disclosure of Users' Private Information was negligent;

b. Whether Defendants owed a duty to Plaintiff and Class Members not to disclose their Private Information to unauthorized third parties;

c. Whether Defendants breached their duty to Plaintiff and Class Members not to disclose their Private Information to unauthorized third parties;

d. Whether Defendants represented to Plaintiff and the Class that they would protect Plaintiff's and Class Members' Private Information;

e. Whether Defendants violated Plaintiff's and Class Members' privacy rights;

f. Whether Defendants' practices violated the FSCA;

g. Whether Defendants' practices violated the FDUTPA;

h. Whether Plaintiff and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law;

i. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

255. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendants' misconduct. Even if Class Members could mount such individual litigation, it would still not be

preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be enhanced, and uniformity of decisions ensured.

256. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants misrepresented that they would disclose personal information only for limited purposes that did not include purposes of delivering advertisements or collecting data for commercial use or supplementing consumer profiles created by data aggregators and advertisers;

b. Whether Defendants' privacy policies misrepresented that they collected and shared User information with third-party service providers only for the limited purpose of providing access to its services;

c. Whether Defendants misrepresented that they had in place contractual and technical protections that limit third-party use of User information and that it would seek User consent prior to sharing Private Information with third parties for purposes other than provision of its services;

d. Whether Defendants misrepresented that any information they receive is stored under the same guidelines as any health entity that is subject to the strict patient data sharing and protection practices set forth in the regulations propounded under HIPAA;

e. Whether Defendants misrepresented that they complied with HIPAA's requirements for protecting and handling Users' PHI;

f. Whether Defendants shared the Private Information that Users provided to Defendants with advertising platforms, including Facebook, without adequate notification or disclosure, and without

Users' consent, in violation of health privacy laws and rules and its own privacy policy;

g. Whether Defendants integrated third-party tracking tools, consisting of automated web beacons ("Pixels") in their website that shared Private Information and User activities with third parties for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;

h. Whether Defendants shared Private Information and activity information with Facebook using Facebook's tracking Pixels on their websites without Users' consent;

i. Whether Facebook used the information that Defendants shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

COUNT ONE
VIOLATION OF FLORIDA SECURITY OF COMMUNICATIONS ACT ("FSCA") Fla. Stat. § 934.01 *et seq.*
(On behalf of Plaintiff and the Florida Subclass)

257. Plaintiff incorporates paragraphs 1 through 242, and 244 through 256 as if fully stated herein.

258. Where there is a reasonable expectation of privacy, absent the consent of all parties, the FSCA prohibits, among other things, the intentional interception or procurement of another person to intercept any wire, oral or electronic communication. Fla. Stat. §§ 934.03(1), 934.03(2)(d).

259. The FSCA prohibits: (1) the interception or procurement of another to intercept any wire, oral or electronic communication; (2) the intentional disclosure of the contents of any wire, oral or electronic communication that the discloser knew or should have known was obtained through the interception of a wire, oral or electronic communication; and (3) the intentional use of the contents of any wire, oral or electronic communication that the discloser knew or should have

known was obtained through the interception of a wire, oral or electronic communication. Fla. Stat. 934.03(1).

260. Any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, a wire, electronic or oral communication in violation of the FSCA is subject to a civil action for, among other things: (a) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (b) punitive damages; and (c) reasonable attorneys' fees and other litigation costs reasonably incurred. Fla. Stat. § 934.10.

261. Under the FSCA, "wire communication" means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications or communications affecting intrastate, interstate, or foreign commerce." Fla. Stat. § 934.02(1).

262. Under the FSCA, "intercept" is defined as the "[a]ural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Fla. Stat. § 934.02(3).

263. Under the FSCA, "contents" in the context of "any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." Fla. Stat. § 934.02(7).

264. Under the FSCA, "person" is defined as "any individual, partnership, association, joint stock company, trust, or corporation." Fla. Stat. § 934.02(5).

265. With some exclusions that do not impact the Plaintiff's claims, under the FSCA, "electronic communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system that affects intrastate, interstate, or foreign commerce . . ." Fla. Stat. 934.02(12).

266. By utilizing and embedding the Pixel on its Web Properties, Defendants intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Florida Class Members contemporaneously including communications regarding the selection of doctors, locations of medical care, specific searches provided by Plaintiff and Class Members for medical conditions, diagnosis and treatment—while navigating the Web Properties.

267. Defendants contemporaneously intercepted these communications without authorization and consent from Plaintiff Prosky and Florida Class Members.

268. Defendants intercepted Plaintiff's and Florida Class Members' communications to contemporaneously learn the meaning of the content of Plaintiff's and Florida Class Members' communications.

269. Plaintiff and Florida Class Members had a justified and reasonable expectation under the circumstances that their electronic communications would not be intercepted.

270. Plaintiff and Florida Class Members were not aware that their electronic communications were being intercepted by Facebook and did not consent to the interception.

271. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

272. Defendants willfully, knowingly, intentionally, and voluntarily engaged in the aforementioned acts when they incorporated the Meta Pixel on their Web Properties, with knowledge of the Pixel's purpose and functionality, and further utilized the benefits that Pixel provides website owners to the detriment of Plaintiff and the Florida Class Members.

273. Plaintiff and the Florida Class Members could not have avoided the harms described herein through the exercise of ordinary diligence.

274. As a result of Defendants' actions, Plaintiff and Florida Class Members have suffered harm and injury.

275. Plaintiff and Florida Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation, including monetary damages.

276. Plaintiff and the Florida Class Members seek appropriate relief for these injuries, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as a result of Defendants' violation of the FSCA.

277. Plaintiff and Florida Class Members seek all other relief as the Court may deem just and proper, including all available monetary relief, injunctive and declaratory relief, any applicable penalties, and reasonable attorneys' fees and costs.

COUNT TWO
VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*
(On behalf of Plaintiff and the Florida Subclass)

278. Plaintiff incorporates paragraphs 1 through 242, and 244 through 256 as if fully stated herein.

279. Florida Statutes Section 501.204 provides that "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are . . . unlawful."

280. Plaintiff Prosky and the Florida Class are "consumers" and "interested persons" as defined in Fla. Stat. 501.203(6)- (7).

281. Defendants engaged in unfair business practices by disclosing Plaintiff Prosky's and Florida Class Members' Private Information to unrelated third parties, including Facebook, without prior consent despite their promises to keep such information confidential.

282. The unfair business practices by Defendants included widespread violations of Plaintiff Prosky's and Florida Class Members' rights to privacy, including their failure to inform the public that using their Web Properties would result in disclosing very private information to a third party.

283. Further, Defendants failed to issue a notice to Plaintiff Prosky and Florida Class Members' that their Private Information was impermissibly being disclosed to an unauthorized third party. In fact, Defendants ***never*** disclosed to Plaintiff Prosky or Florida Class Members that they shared their sensitive and confidential communications and Private Information with Facebook and other third parties.[87]

[87] In contrast to Defendants, several medical providers which have installed the Meta Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, available at https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited May 21, 2024); Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (Oct. 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

284. Plaintiff and the Class Members received and paid for health care services from Defendants.

285. Plaintiff Prosky and the Florida Class Members reasonably relied upon the representations Defendant(s) made in their Privacy Policy, including those representations concerning the confidentiality of patient information.

286. Defendants were in sole possession of and had a duty to disclose the material information that Plaintiff Prosky's and Florida Class Members' Private Information was being shared with a third party.

287. Plaintiff and Florida Class Members would not have utilized Defendants' medical services and/or used their Websites or would have paid much less for Defendants' services had they known that their Private Information would be captured and disclosed to third parties like Facebook without consent.

288. As a direct and proximate cause of Defendants' actions, Plaintiff Prosky and Florida Class Members suffered actual damages.

289. The harm caused by Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests other than the wrongful conduct described herein.

290. Defendants knew or should have known of their deceptive, unfair, and unlawful conduct of disclosing Plaintiff Prosky's and Florida Class Members' Private Information to unauthorized third parties.

291. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

overpaying for Defendants' health care services and loss of value of their personally identifiable patient data and communications.

292. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiff and the Class Members were also damaged by Defendants' conduct in that:

a. Defendants harmed Plaintiff's and Class Members' interest in privacy;
b. Sensitive and confidential information that Plaintiff and Class Members intended to remain private has been disclosed to third parties;
c. Defendants eroded the essential confidential nature of the provider-patient relationship;
d. Defendants took something of value from Plaintiff and Class Members, i.e., their personally identifiable patient information, and derived a benefit therefrom without Plaintiff's or the Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;
e. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality; and
f. Defendants' actions diminished the value of Plaintiff's and Class Members' personal information.

293. Pursuant to Florida Statutes Section 501.211(2), Plaintiff Prosky and the Florida Class seek actual damages, plus attorneys' fees and costs.

294. Pursuant to Florida Statutes Section 501.211(1), Plaintiff Prosky and the Florida Class seek declaratory judgment that the above-described wrongful acts violate the FDUTPA.

295. Plaintiff Prosky and the Florida Class also seek injunctive relief in the form of an order against Defendants to prevent them from sharing Plaintiff Prosky's and the Florida Class Members' Private Information among themselves and other third parties.

COUNT THREE
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA") 18 U.S.C. § 2511, *et seq.*
Unauthorized Interception, Use, and Disclosure
(On behalf Plaintiff and the Nationwide Class)

296. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

297. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

298. The ECPA protects both sending and receipt of communications.

299. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

300. The transmissions of Plaintiff's Private Information to Defendants' Web Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

301. **Electronic Communications.** The transmission of Private Information between Plaintiff and Class Members and Defendants' Web Properties with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

302. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

303. Defendants' intercepted communications include, but are not limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, specific searches

for diagnosis of certain conditions, treatment/medication for such conditions, and the search for doctors, appointments, and locations for treatment. Furthermore, Defendants intercepted the "contents" of Plaintiff's communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. Personally identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions, including but not limited to cardiac-related issues;

f. The precise text of information generated when patients requested or made appointments;

g. The precise text of patient communications about specific treatments;

h. The precise text of patient communications about scheduling appointments with medical providers;

i. The precise text of patient communications about billing and payment;

j. The precise text of specific buttons on Defendants' Websites that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

k. The precise dates and times when patients click to Log-In on Defendants' Websites;

l. The precise dates and times when patients visit Defendants' Websites;

m. Information that is a general summary or informs third parties of the general subject of communications that Defendants send back to patients in response to search queries and requests for information

about specific doctors, conditions, treatments, billing, payment, and other information.

304. For example, Defendants' interceptions of the fact that a patient views a webpage like:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

305. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

306. **Electronical, Mechanical or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendants' web-servers; and

d. The Pixel code deployed by Defendants to effectuate the sending and acquisition of patient communications.

307. By utilizing and embedding the Pixel on their Web Properties, Defendants intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiff and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

308. Specifically, Defendants intercepted Plaintiff's and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiff's and Class Members' Private Information to third parties such as Facebook.

309. 296. This information was, in turn, used by third parties, such as Facebook to 1) place Plaintiff and Class Members in specific health-related categories and 2) target Plaintiff and Class Members with advertising associated with their specific health conditions.

310. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(c).

311. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendants violated 18 U.S.C. § 2511(1)(d).

312. Unauthorized Purpose. Defendants intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

313. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

314. Defendants are not a party to the communications based on their unauthorized duplication and transmission of communications with Plaintiff and the Nationwide Class. However, even assuming Defendants are a party, Defendants' simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

315. 301. Defendants are not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiff and the Class. However, even assuming Defendants are a party, Defendants simultaneous, unknown duplication, forwarding, and interception of Plaintiff's and Class Members' Private Information does not qualify for the party exemption.

316. Here, as alleged above, Defendants violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party.

317. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

318. 304. Plaintiff's and Class Members' information that Defendants disclosed to third parties qualifies as IIHI, and Defendants violated Plaintiff's expectations of privacy, and

constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendants intentionally used the wire or electronic communications to intercept Plaintiff's Private Information in violation of the law.

319. Defendants' conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to Facebook without patient authorization.

320. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

321. Defendants' conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendants' use of the Facebook source code was for Defendants' commercial advantage to increase revenue from existing patients and gain new patients.

322. Defendants' acquisition of patient communications that were used and disclosed to Facebook was also done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Violations of the FDUTPA;

b. Violation of the FSCA;

c. Invasion of Privacy/Intrusion upon Seclusion;

d. Negligence;

e. Breach of Confidence;

f. Breach of implied contract; and

g. Breach of fiduciary duty.

323. Defendants are not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that they were participants in Plaintiff's and Class Members' communications about their Private Information on their Web Properties, because they used their participation in these communications to improperly share Plaintiff's and Class Members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiff and Class Members did not know third parties were receiving their information, and that Plaintiff and Class Members did not consent to receive this information.

324. Here, as alleged above, Defendants violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information to a third party.

325. As such, Defendants cannot viably claim any exception to ECPA liability.

326. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendants' invasion of privacy in that:

a. Learning that Defendants have intruded upon, intercepted, transmitted, shared, and used their Private Information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and Class Members to suffer emotional distress;

b. Defendants received substantial financial benefits from their use of Plaintiff's and Class Members' Private Information without providing any value or benefit to Plaintiff or Class Members;

c. Defendants received substantial, quantifiable value from their use of Plaintiff's and Class Members' Private Information, such as understanding how people use their Web Properties and determining what ads people see on their Web Properties, without providing any value or benefit to Plaintiff or Class Members;

d. Defendants have failed to provide Plaintiff and Class Members with the full value of the medical services for which they paid, which

included a duty to maintain the confidentiality of their patient information; and

e. The diminution in value of Plaintiff's and Class Members' Private Information and the loss of privacy due to Defendants making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiff and Class Members intended to remain private no longer private.

327. Defendants intentionally used the wire or electronic communications to increase their profit margins. Defendants specifically used the Pixel to track and utilize Plaintiff's and Class Members' Private Information for financial gain.

328. Defendants were not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

329. Plaintiff and Class Members did not authorize Defendants to acquire the content of their communications for purposes of invading their privacy via the Pixel.

330. Any purported consent that Defendants received from Plaintiff and Class Members was not valid.

331. Consumers have the right to rely upon the promises that companies make to them. Defendants accomplished their tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiff's and Class members' computing devices as "first-party" cookies that are not blocked.

332. Defendant's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below; and

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Facebook.

333. Defendants acted with the intent to defraud in that they willfully invaded and took Plaintiff's and Class Members' property:

a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

334. In sending and in acquiring the content of Plaintiff's and Class Members' communications relating to the browsing of Defendants' Web Properties, Defendants' purpose was tortious, criminal, and designed to violate federal and state legal provisions including a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

335. As a result of Defendants' violation of the ECPA, Plaintiff and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT FOUR
INVASION OF PRIVACY
INTRUSION UPON SECLUSION
(On behalf of Plaintiff and the Nationwide Class)

336. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

337. Plaintiff and Nationwide Class Members had a reasonable and legitimate expectation of privacy in the Private Information that Defendants failed to adequately protect against disclosure from unauthorized parties.

338. Defendants owed a duty to Plaintiff and Nationwide Class Members to keep their Private Information confidential.

339. Defendants failed to protect and release to unknown and unauthorized third parties the Private Information of Plaintiff and Nationwide Class Members.

340. By failing to keep Plaintiff's and Nationwide Class Members' Private Information confidential and safe from misuse, Defendants knowingly sharing highly sensitive Private Information with Facebook, Defendants unlawfully invaded Plaintiff's and Nationwide Class Members' privacy by, among others: (i) intruding into Plaintiff's and Nationwide Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons; and (iii) enabling and facilitating the disclosure of Plaintiff's and Class Members' Private Information without authorization or consent.

341. Plaintiff's and Nationwide Class Members' expectation of privacy was and is especially heightened given Defendants' consistent representations that Users' information would remain confidential and would not be disclosed to anyone without User consent.

342. Defendants' privacy policy specifically provides, "Palm Beach Gardens Medical Center and its affiliates ("we," "our" or "us") are committed to protecting your privacy, so we have adopted privacy practices to protect the information we collect from you."[88]

[88] *Privacy Policy,* PALM BEACH GARDENS MEDICAL CENTER, https://www.pbgmc.com/privacy-policy#:~:text=We%20do%20not%20sell%20personal,consumers%20to%20any%20third%20parties.&text=We%20may%20collect%20certain%20information%20by%20automated%20means. (last visited May 21, 2024).

343. Defendants knew, or acted with reckless disregard of the fact that a reasonable person in Plaintiff's and Nationwide Class Members' position would consider their actions highly offensive.

344. Defendants' unauthorized surreptitious recording, monitoring, and sharing of the Users' activities, searches, researching diagnosis and treatment, searching for doctors and medical specialists violated expectations of privacy that have been established by social norms.

345. As a proximate result of such unauthorized disclosures, Plaintiff's and Nationwide Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted and caused damages to Plaintiff and Nationwide Class Members.

346. Plaintiff and Nationwide Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional natura of Defendants' conduct, directed at injuring Plaintiff and Nationwide Class Members in conscious disregard of their rights.

347. Plaintiff seeks injunctive relief on behalf of the Nationwide Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause irreparable injury to Plaintiff and Nationwide Class Members. Plaintiff and Nationwide Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Nationwide Class.

COUNT FIVE
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

348. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

349. When Plaintiff and Nationwide Class Members provided their Private Information to Defendants in exchange for services, they entered into implied contracts by which Defendants agreed to safeguard and not disclose such Private Information without consent.

350. Plaintiff and Nationwide Class Members accepted Defendants' offers of services and provided their Private Information to Defendants via the Web Properties.

351. Plaintiff and Nationwide Class Members would not have entrusted Defendants with their Private Information in the absence of an implied contract between them that included Defendants' promise not to disclose Private Information without consent.

352. Defendants breached these implied contracts by disclosing Plaintiff's and Nationwide Class Members' Private Information to third parties, including Facebook.

353. As a direct and proximate result of Defendants' breaches of these implied contracts, Plaintiff and Nationwide Class Members sustained damages as alleged herein. Plaintiff and Nationwide Class Members would not have used Defendants' services, or would have paid substantially less for these services, had they known their Private Information would be disclosed.

354. Plaintiff and Nationwide Class Members are entitled to compensatory and consequential damages as a result of Defendants' breach of implied contract.

COUNT SIX
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

355. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

356. Defendants owed a duty to Plaintiff and the Nationwide Class to exercise due care in collecting, storing, safeguarding, and preventing any disclosure of their Private Information. This duty included but was not limited to: (a) preventing Plaintiff's and Nationwide Class Members' Private Information from being to be disclosed to unauthorized third parties; and (b)

destroying Plaintiff's and Nationwide Class Members' Private Information within an appropriate amount of time after it was no longer required by Defendants.

357. Defendants' duties to use reasonable care arose from several sources, including those described below. Defendants had a common law duty to prevent foreseeable harm to others, including Plaintiff and Nationwide Class Members, who were the foreseeable and probable victims of any data misuse, such as disclosure of Private Information to unauthorized parties.

358. Defendants had a special relationship with Plaintiff and Nationwide Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Nationwide Class Members resulting from unauthorized disclosure of their Private Information to third parties such as Facebook. Plaintiff and Nationwide Class Members were compelled to entrust Defendants with their Private Information. At relevant times, Plaintiff and Nationwide Class Members understood that Defendants would take adequate data storage practices to safely store their Private Information. Only Defendants had the ability to protect Plaintiff's and Nationwide Class Members' Private Information collected and stored on Defendants' websites.

359. Defendants' duty to use reasonable measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of [PHI]." 45 C.F.R. § 164.530(c)(1).

360. Defendants' conduct as described above constituted an unlawful breach of their duty to exercise due care in collecting, storing, and safeguarding Plaintiff's and the Nationwide Class Members' Private Information by failing to protect this information.

361. Plaintiff and Nationwide Class Members trusted Defendants and in doing so provided Defendants with their Private Information, based upon Defendants' representations that they would "take reasonable, industry standard precautions to keep the Sites and their systems secure and to prevent personal information from being made available to unauthorized persons or entities."[89] Defendants failed to do so.

362. Defendants breached their duty in this relationship to collect and safely store Plaintiff's and Nationwide Class Members' Private Information.

363. Plaintiff's and the Nationwide Class Members' Private Information would have remained private and secure had it not been for Defendants' wrongful and negligent breach of their duties. Defendants' negligence was, at least, a substantial factor in causing Plaintiff's and Nationwide Class Members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Plaintiff and the Nationwide Class Members other injuries because of the unauthorized disclosures.

364. The damages suffered by Plaintiff and the Nationwide Class Members were the direct and reasonably foreseeable result of Defendants' negligent breach of their duties to maintain Users' Private Information. Defendants knew or should have known that their unauthorized disclosure of highly sensitive Private Information was a breach of their duty to collect and safely store such information.

365. Defendants' negligence directly caused significant harm to Plaintiff and the Nationwide Class. Specifically, Plaintiff and Nationwide Class Members are now subject to their sensitive information being accessed by unauthorized parties, which may lead to significant harms.

[89] *Notice of Privacy Practices*, https://www.palmbeachhealthnetwork.com/notice-of-privacy-practices (last visited May 21, 2024).

366. Plaintiff hereby incorporates all other paragraphs as if fully stated herein.

367. Defendants had a fiduciary duty to protect the confidentiality of their communications with Plaintiff and Nationwide Class Members by virtue of the explicit privacy representations Defendants made on their websites to Plaintiff and members of the Nationwide Class.

368. Defendants had information relating to Plaintiff and Nationwide Class Members that they knew or should have known to be confidential.

369. Plaintiff's and Nationwide Class Members' communications with Defendants about sensitive Private Information and their status as patients of Defendants were not matters of general knowledge.

370. Defendants breached their fiduciary duty of confidentiality by designing their data protection systems in a way to allow for a data breach of a massive caliber.

371. At no time did Plaintiff or Nationwide Class Members give informed consent to Defendants' conduct.

372. As a direct and proximate cause of Defendants' actions, Plaintiff and Nationwide Class Members suffered damage in that the information they intended to remain private is no longer so and their Private Information was disclosed to, tracked, and intercepted by third-party Internet tracking companies, including Facebook, without their knowledge or consent.

COUNT SEVEN
BREACH OF CONFIDENCE
(*On Behalf of Plaintiff and the Nationwide Class*)

373. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

374. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

375. Plaintiff and Nationwide Class Members had reasonable expectations of privacy in their communications exchanged with Defendants, including communications exchanged on Defendants' Websites.

376. Plaintiff's and Nationwide Class Members' reasonable expectations of privacy in the communications exchanged with Defendants were further solidified by Defendants' express promises in their Privacy Policies.

377. Contrary to their duties as a medical provider and their express promises of confidentiality, Defendants deployed the Pixel (and other tracking technologies) to disclose and transmit Plaintiff's and Nationwide Class Members' Private Information and the contents of their communications exchanged with Defendants to third parties.

378. The third-party recipients included, but were not limited to, Facebook and other online marketers.

379. Defendants' disclosures of Plaintiff's and Nationwide Class Members' Private Information were made without their knowledge, consent or authorization, and were unprivileged.

380. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

381. As a direct and proximate cause of Defendants' unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiff and Nationwide Class Members were damaged by Defendants' breach in that:

a. Sensitive and confidential information that Plaintiff and Nationwide Class Members intended to remain private is no longer private;

b. Defendants eroded the essential confidential nature of the provider-patient relationship;

c. Defendants took something of value from Plaintiff and Nationwide Class Members and derived benefit therefrom without Plaintiff's and Nationwide Class Members' knowledge or informed consent and without compensating Plaintiff and Nationwide Class Members for the data;

d. Plaintiff and Nationwide Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality;

e. Defendants' actions diminished the value of Plaintiff's and Nationwide Class Members' Private Information; and

f. Defendants' actions violated the property rights Plaintiff and Nationwide Class Members have in their Private Information.

382. Plaintiff and Nationwide Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation. Plaintiff is also entitled to punitive damages.

COUNT EIGHT
BREACH OF FIDUCIARY DUTY
(*On Behalf of Plaintiff and the Nationwide Class*)

383. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

384. In light of the special relationship between Defendants, Plaintiff and Nationwide Class Members, whereby Defendants became guardian of Plaintiff's and Nationwide Class Members' Private Information, Defendants became a fiduciary by their undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Nationwide Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Nationwide Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and do store.

385. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Nationwide Class Members upon matters within the scope of Defendants' relationship with their patients and former patients, in particular, to keep secure their Private Information.

386. Defendants breached their fiduciary duties to Plaintiff and Nationwide Class Members by disclosing their Private Information to unauthorized third parties, and separately, by failing to notify Plaintiff and Nationwide Class Members of this fact.

387. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Nationwide Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT NINE
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

388. Plaintiff incorporates paragraphs 1 through 256 as if fully stated herein.

389. Plaintiff pleads unjust enrichment in the alternative to his breach of contract claims.

390. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Defendants knowingly realized millions of dollars in revenue from the use of the Private Information of Plaintiff and Class Members for profit by way of targeted advertising related to Users' respective medical conditions and treatments sought.

391. This Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon Defendants by Plaintiff and Class Members.

392. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

393. It would be inequitable and unjust to permit Defendants to retain the enormous economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiff and Class Members.

394. Defendants will be unjustly enriched if they are permitted to retain the economic benefits conferred upon them by Plaintiff and Class Members through Defendants' obtaining the Private Information and the value thereof, and profiting from the unlawful, unauthorized and impermissible use of the Private Information of Plaintiff and Class Members.

395. Plaintiff and Class Members are therefore entitled to recover the amounts realized by Defendants at the expense of Plaintiff and Class Members.

396. Plaintiff and Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to the recover the amount of Defendants' ill-gotten gains, and/or other sums as may be just and equitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the Proposed Classes defined herein, respectfully request:

A. That this Action be maintained as a Class Action, that Plaintiff be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

i. Preventing Defendants from sharing Plaintiff's and Class Members' Private Information among themselves and other third parties;

ii. Requiring Defendants to alert and/or otherwise notify all users of their websites and portals of what information is being collected, used, and shared;

iii. Requiring Defendants to provide clear information regarding their practices concerning data collection from the users/patients of Defendants' Web Properties, as well as uses of such data;

iv. Requiring Defendants to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

v. Requiring Defendants to provide an opt out procedures for individuals who do not wish for their information to be tracked while interacting with Defendants' Web Properties;

vi. Mandating the proper notice be sent to all affected individuals, and posted publicly;

vii. Requiring Defendants to delete, destroy, and purge the Private Information of Users unless Defendants can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

viii. Requiring all further and just corrective action, consistent with permissible law.

C. That the Court award Plaintiff and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendants to which Plaintiff and the Class are entitled, including but not limited to restitution;

E. Plaintiff and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiff and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiff and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any other relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

DATED: May 22, 2024

CLARKSON LAW FIRM, P.C.

By: */s/ Matthew J. Langley*

Matthew J. Langley
Florida Bar No. 97331
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
matt@almeidalawgroup.com

Ryan Clarkson (*pro hac vice* forthcoming)
Yana Hart (*pro hac vice* forthcoming)

Tiara Avaness (*pro hac vice* forthcoming)
CLARKSON LAW FIRM, P.C.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (231) 788-4070
rclarkson@clarksonlawfirm.com
yhart@clarksonlawfirm.com
tavaness@clarksonlawfirm.com

Attorneys for Plaintiff and the Class